PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #95

Browse in private

If you don’t want Google Chrome to remember your activity, you can browse the web privately in Incognito mode.

Computer Android iPhone & iPad

1. On your computer, open Chrome.
2. At the top right, click More ⋮ > **New Incognito Window**.
3. A new window appears. In the top corner, check for the Incognito icon.

You can also use a keyboard shortcut to open an Incognito window:

- Windows, Linux, or Chrome OS: Press **Ctrl + Shift + n**.
- Mac: Press ⌘ **+ Shift + n**.

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

You can also choose to block third-party cookies when you open a new Incognito window. Learn more about cookies.

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ×.
   - **Mac:** At the top left, click Close ×.

What happens when you browse privately

- Chrome doesn't save your browsing history, cookies and site data, or information entered in forms.
- Files you download and bookmarks you create are kept.
- Your activity isn’t hidden from websites you go to, your employer or school, or your internet service provider.

Learn more about how private browsing works.

Related articles

- How private browsing works
- Let others browse Chrome as a guest
- Clear Chrome browsing data

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #96

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new Incognito window. Learn more about cookies.

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won’t save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you’re using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session. When you search on Google, Google will always estimate the general area that you're searching from. Learn more about location when you search on Google.

Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify the general area you're in
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can’t change your saved info in a Chrome Incognito window.

Downloads and bookmarks are saved

Chrome won’t store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

Computer Android iPhone & iPad

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

You can also choose to block third-party cookies when you open a new Incognito window. Learn more about cookies.

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ×.
   - **Mac:** At the top left, click Close ×.

Related articles

- Browse in private
- Let others browse Chrome as a guest
- Clear Chrome browsing data

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #116

Perma.cc record

Captured May 26, 2022 4:59 pm

View: Standard (/Q5JW-H45J?type=standard) Screenshot (/Q5JW-H45J?type=image)

Show record details

View the live page (https://support.google.com/chrome/answer/7440301?hl=en)

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new incognito window. Learn more about cookies.

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won’t save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you’re using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session. When you search on Google, Google will

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #160

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new Incognito window. Learn more about cookies.

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session. When you search on Google, Google will always estimate the general area that you're searching from. Learn more about location when you search on Google.

Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify the general area you're in
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

Computer Android iPhone & iPad

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

You can also choose to block third-party cookies when you open a new Incognito window. Learn more about cookies.

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ×.
   - **Mac:** At the top left, click Close ×.

Related articles

- Browse in private
- Let others browse Chrome as a guest
- Clear Chrome browsing data

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #161

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.

Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify your general location
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

Computer Android iPhone & iPad

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

Stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ✕ .
   - **Mac:** At the top left, click Close ✕ .

Related articles

- Browse in private
- Let others browse Chrome as a guest
- Clear Chrome browsing data

Was this helpful?

Yes No

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #163

Documentation > Chrome DevTools > Network

Inspect network activity

Published on Friday, February 8, 2019

Get started Find issues

Kayce Basques
Technically, I'm a writer
Twitter GitHub Glitch

Table of contents ▾

This is a hands-on tutorial of some of the most commonly-used DevTools features related to inspecting a page's network activity.

See Network Reference if you'd like to browse features instead.

Read on, or watch the video version of this tutorial:

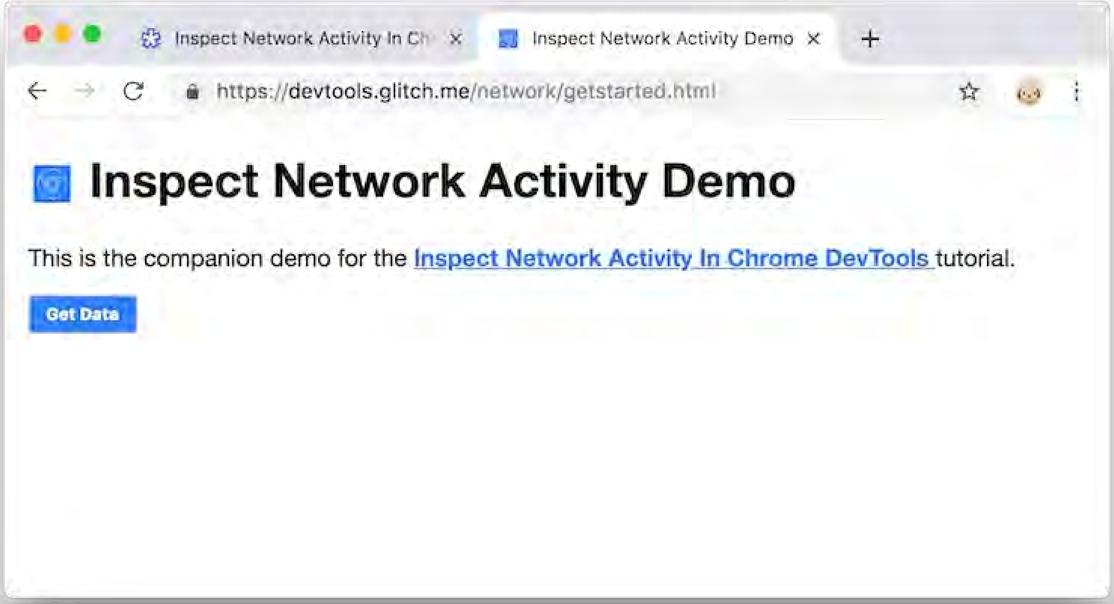
When to use the Network panel

In general, use the Network panel when you need to make sure that resources are being downloaded or uploaded as expected. The most common use cases for the Network panel are:

- Making sure that resources are actually being uploaded or downloaded at all.
- Inspecting the properties of an individual resource, such as its HTTP headers, content, size, and so on.

If you're looking for ways to improve page load performance, *don't* start with the Network panel. There are many types of load performance issues that aren't related to network activity. Start with the Audits panel because it gives you targeted suggestions on how to improve your page. See Optimize Website Speed.

1 Open the Get Started Demo.

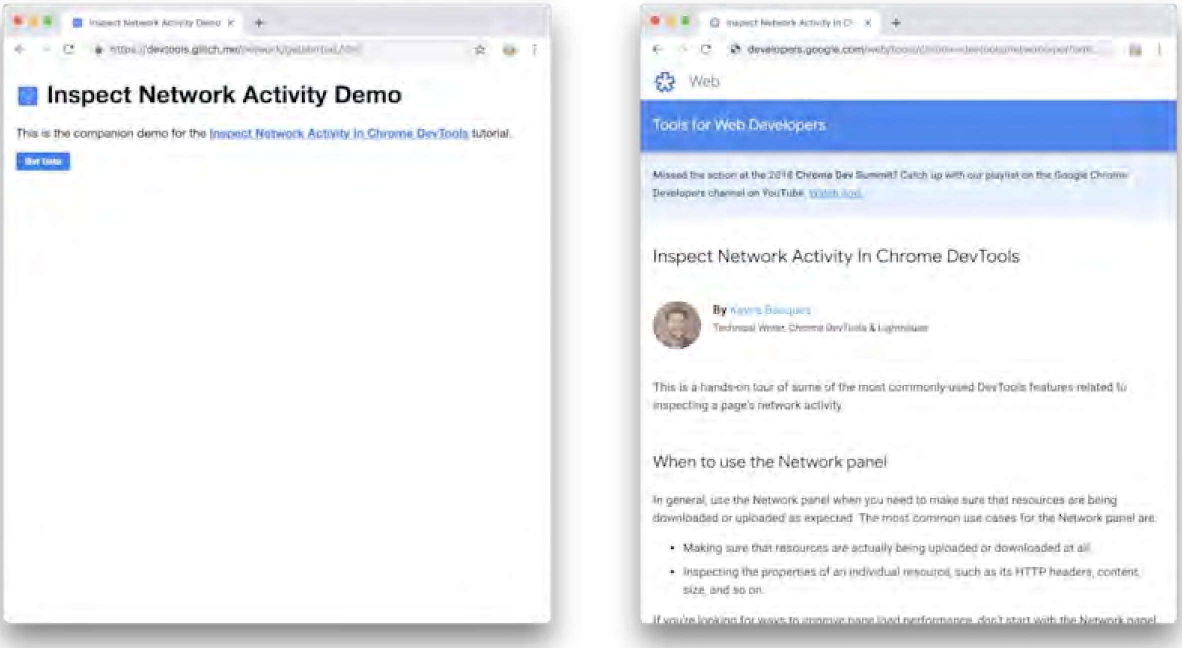

Inspect Network Activity In Ch ×
Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Figure 1. The demo

You might prefer to move the demo to a separate window.


Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data
Inspect Network Activity In Ch ×
developers.google.com/web/tools/chrome-devtools/network/performance
Web

Tools for Web Developers

Missed the action at the 2018 Chrome Dev Summit? Catch up with our playlist on the Google Chrome Developers channel on YouTube. Watch now.

Inspect Network Activity In Chrome DevTools

By Kayce Basques
Technical Writer, Chrome DevTools & Lighthouse

This is a hands-on tour of some of the most commonly-used DevTools features related to inspecting a page's network activity.

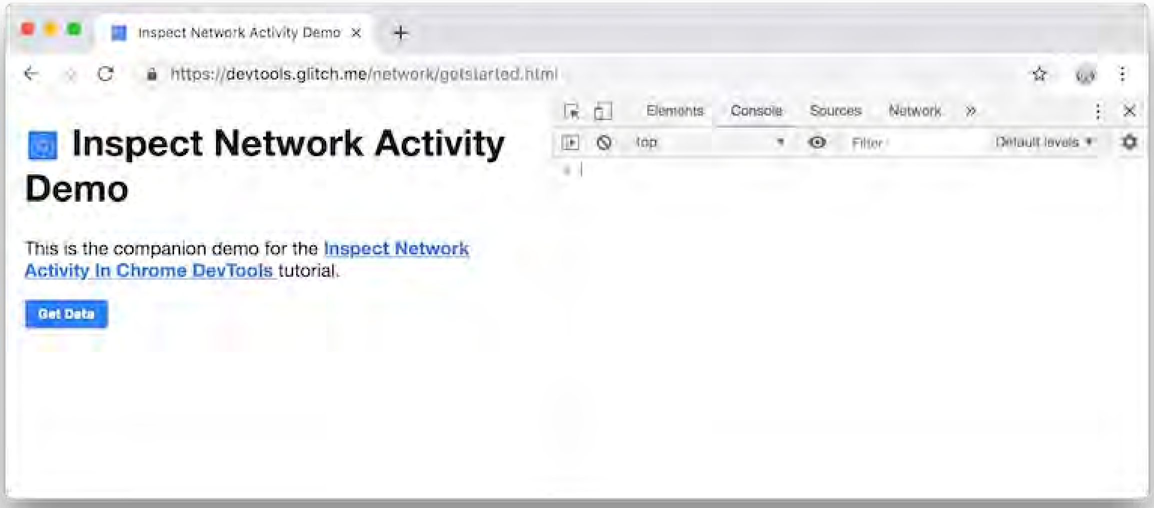
When to use the Network panel

In general, use the Network panel when you need to make sure that resources are being downloaded or uploaded as expected. The most common use cases for the Network panel are:

- Making sure that resources are actually being uploaded or downloaded at all.
- Inspecting the properties of an individual resource, such as its HTTP headers, content, size, and so on.

If you're looking for ways to improve page load performance, don't start with the Network panel.

Figure 2. The demo in one window and this tutorial in a different window

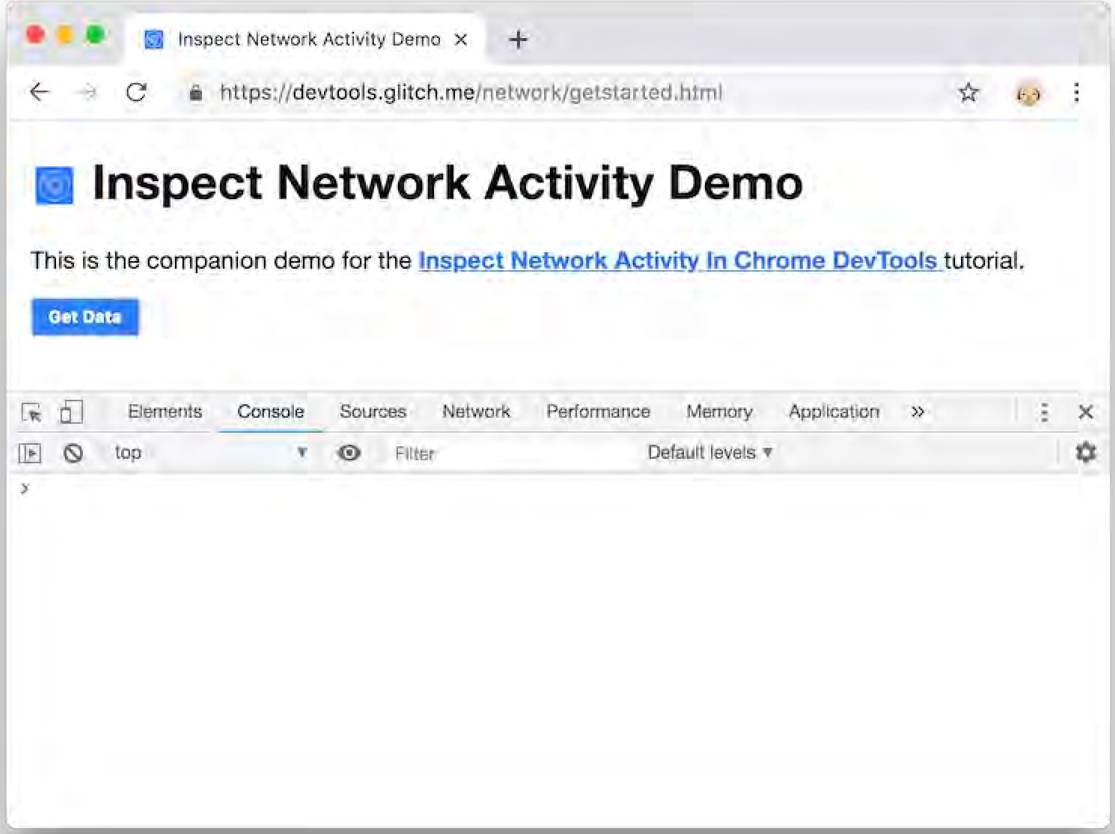

Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Elements
Console
Sources
Network
top
Filter
Default levels

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

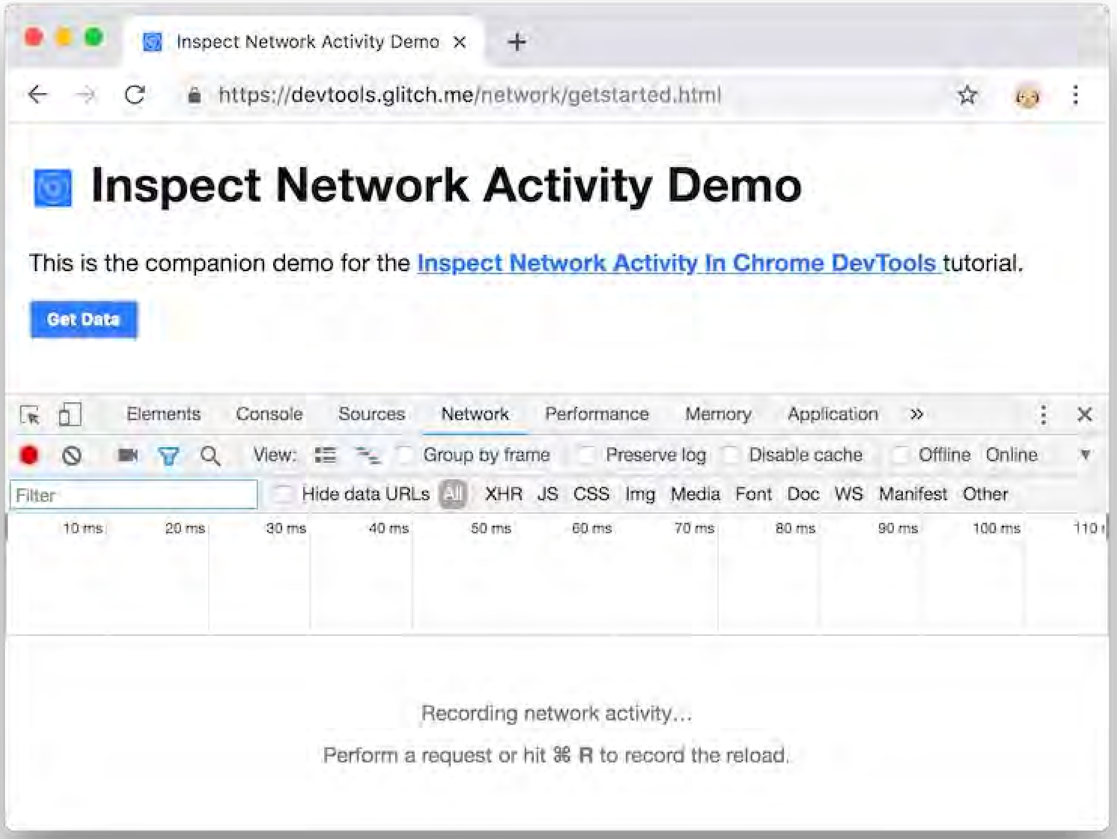
Figure 3. The Console

You might prefer to dock DevTools to the bottom of your window.


Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Recording network activity...

Perform a request or hit ⌘ R to record the reload.

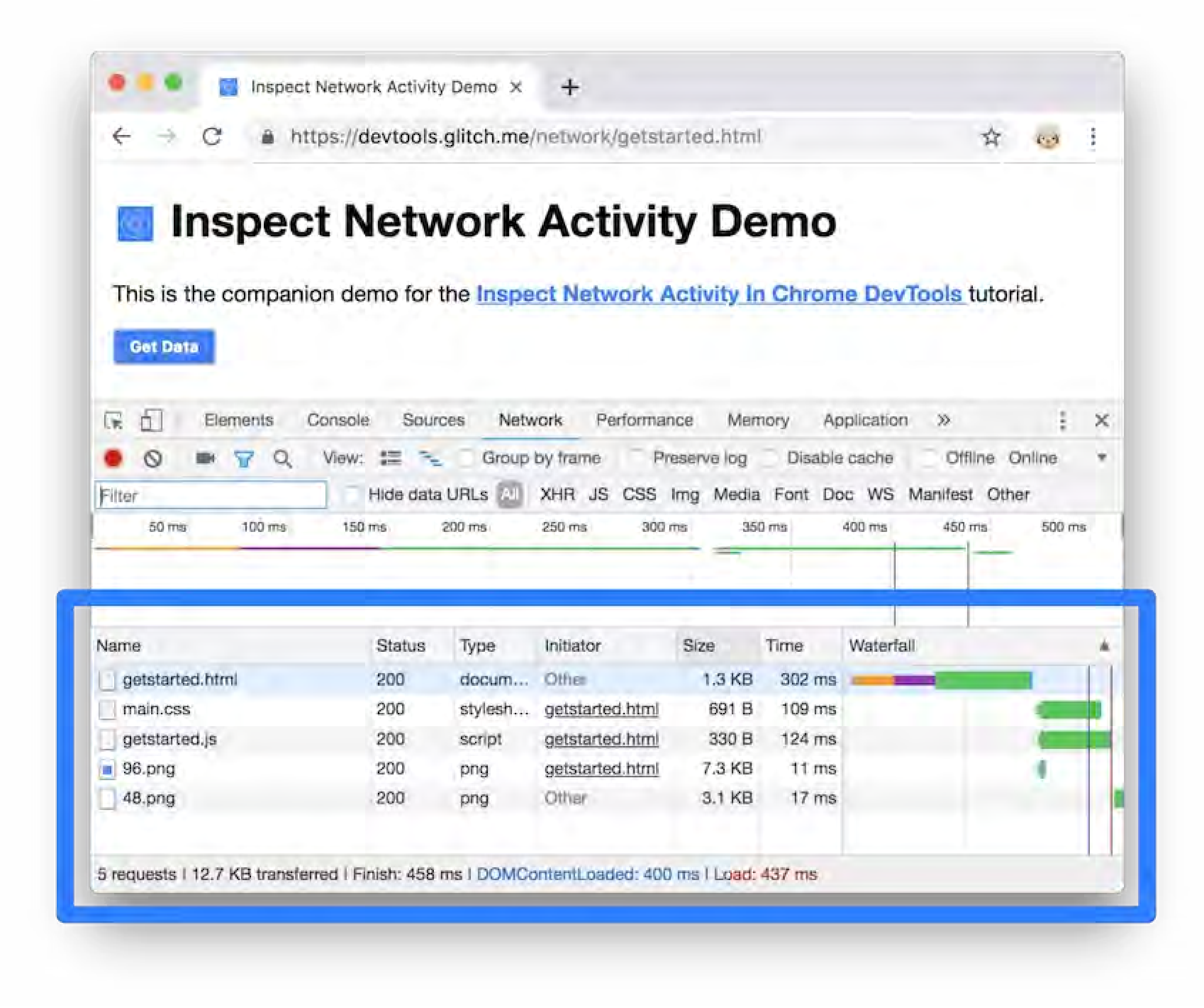
Figure 5. DevTools docked to the bottom of the window

Right now the Network panel is empty. That's because DevTools only logs network activity while it's open and no network activity has occurred since you opened DevTools.

Log network activity

To view the network activity that a page causes:

1. Reload the page. The Network panel logs all network activity in the **Network Log**.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum...	Other	1.3 KB	302 ms	
main.css	200	stylesh...	getstarted.html	691 B	109 ms	
getstarted.js	200	script	getstarted.html	330 B	124 ms	
96.png	200	png	getstarted.html	7.3 KB	11 ms	
48.png	200	png	Other	3.1 KB	17 ms	

5 requests | 12.7 KB transferred | Finish: 458 ms | DOMContentLoaded: 400 ms | Load: 437 ms

Figure 6. The Network Log

Each row of the **Network Log** represents a resource. By default the resources are listed chronologically. The top resource is usually the main HTML document. The bottom resource is whatever was requested last.

Each column represents information about a resource. **Figure 6** shows the default columns:

Status. The HTTP response code.

Type. The resource type.

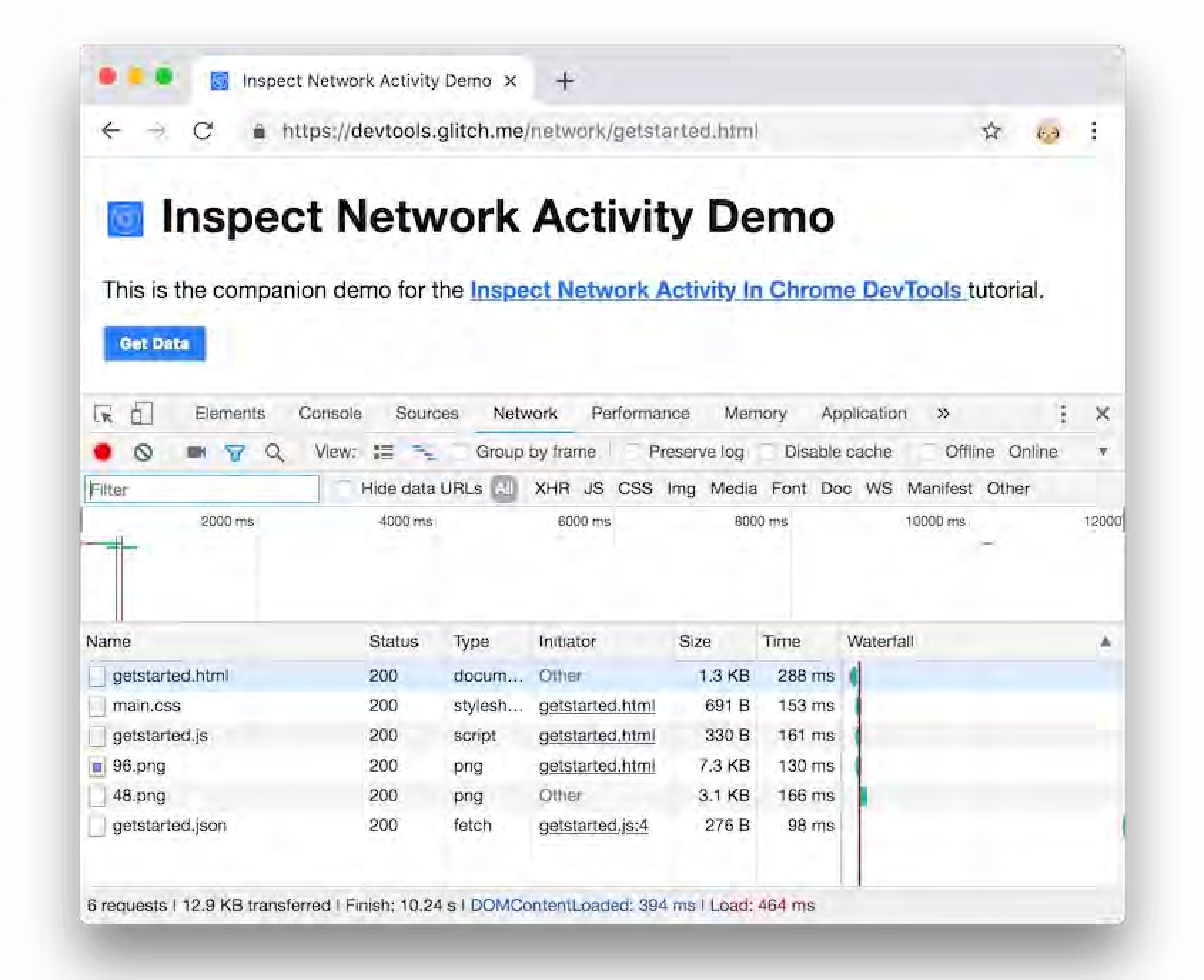
Initiator. What caused a resource to be requested. Clicking a link in the Initiator column takes you to the source code that caused the request.

Note The graph above the Network Log is called the Overview. You won't be using it in this tutorial, so you can hide it if you prefer. See Hide the Overview pane.

2 So long as you've got DevTools open, it will record network activity in the Network Log. To demonstrate this, first look at the bottom of the **Network Log** and make a mental note of the last activity.

3 Now, click the **Get Data** button in the demo.

4 Look at the bottom of the **Network Log** again. There's a new resource called `getstarted.json`. Clicking the **Get Data** button caused the page to request this file.



Inspect Network Activity Demo

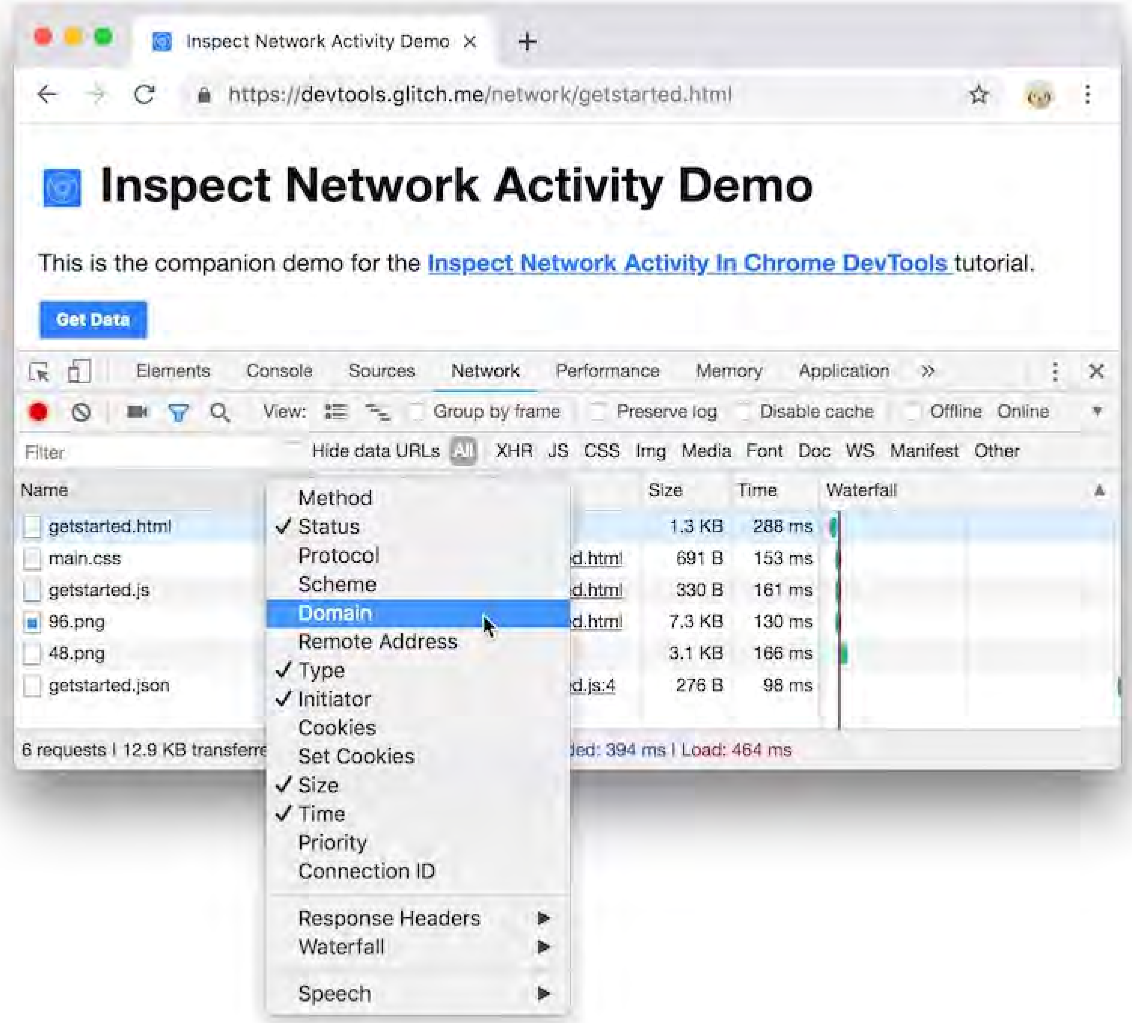
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum...	Other	1.3 KB	288 ms	
main.css	200	stylesh...	getstarted.html	691 B	153 ms	
getstarted.js	200	script	getstarted.html	330 B	161 ms	
96.png	200	png	getstarted.html	7.3 KB	130 ms	
48.png	200	png	Other	3.1 KB	166 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	98 ms	

6 requests | 12.9 KB transferred | Finish: 10.24 s | DOMContentLoaded: 394 ms | Load: 464 ms

The columns of the Network Log are configurable. You can hide columns that you're not using. There are also many columns that are hidden by default which you may find useful.

1 Right-click the header of the Network Log table and select **Domain**. The domain of each resource is now shown.



Inspect Network Activity Demo

https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name		Size	Time	Waterfall
getstarted.html		1.3 KB	288 ms	
main.css	d.html	691 B	153 ms	
getstarted.js	d.html	330 B	161 ms	
96.png	d.html	7.3 KB	130 ms	
48.png		3.1 KB	166 ms	
getstarted.json	d.js:4	276 B	98 ms	

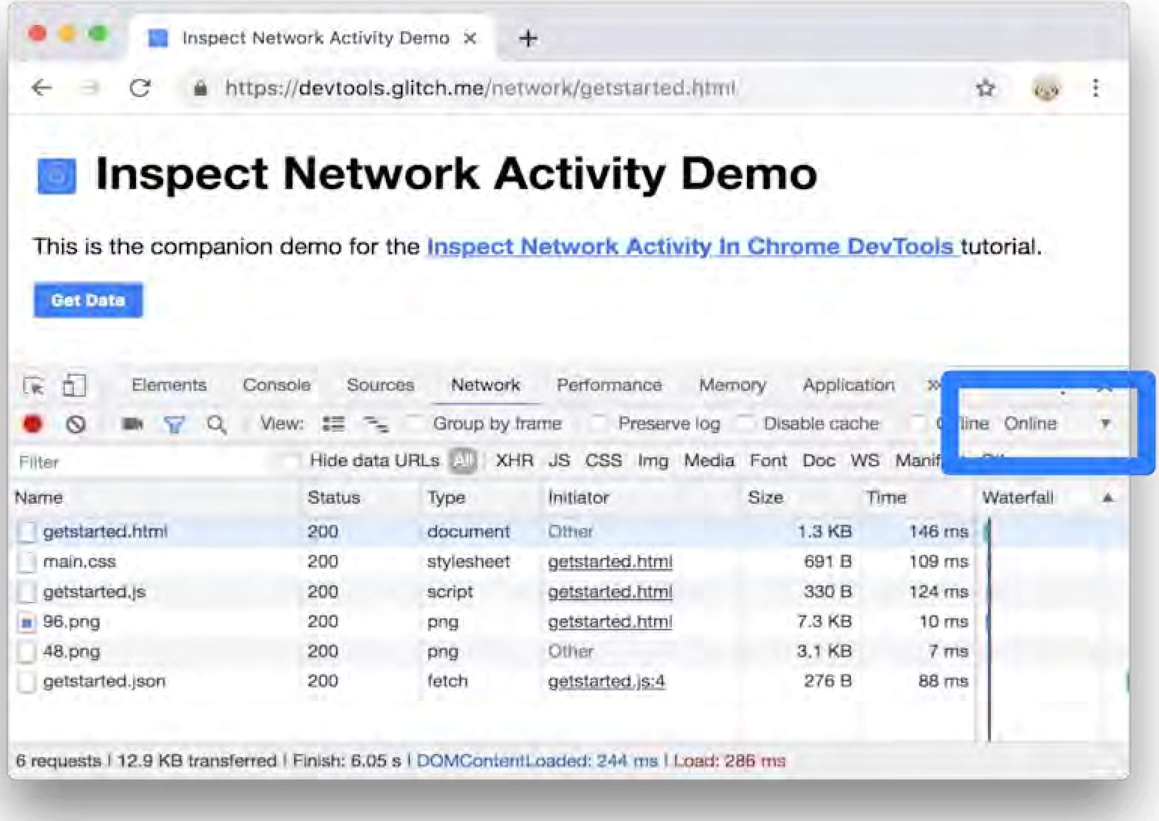
6 requests | 12.9 KB transferre … ded: 394 ms | Load: 464 ms

Figure 8. Enabling the Domain column

Tip You can see the full URL of a resource by hovering over its cell in the **Name** column.

The network connection of the computer that you use to build sites is probably faster than the network connections of the mobile devices of your users. By throttling the page you can get a better idea of how long a page takes to load on a mobile device.

1 Click the **Throttling** dropdown, which is set to **Online** by default.



Inspect Network Activity Demo

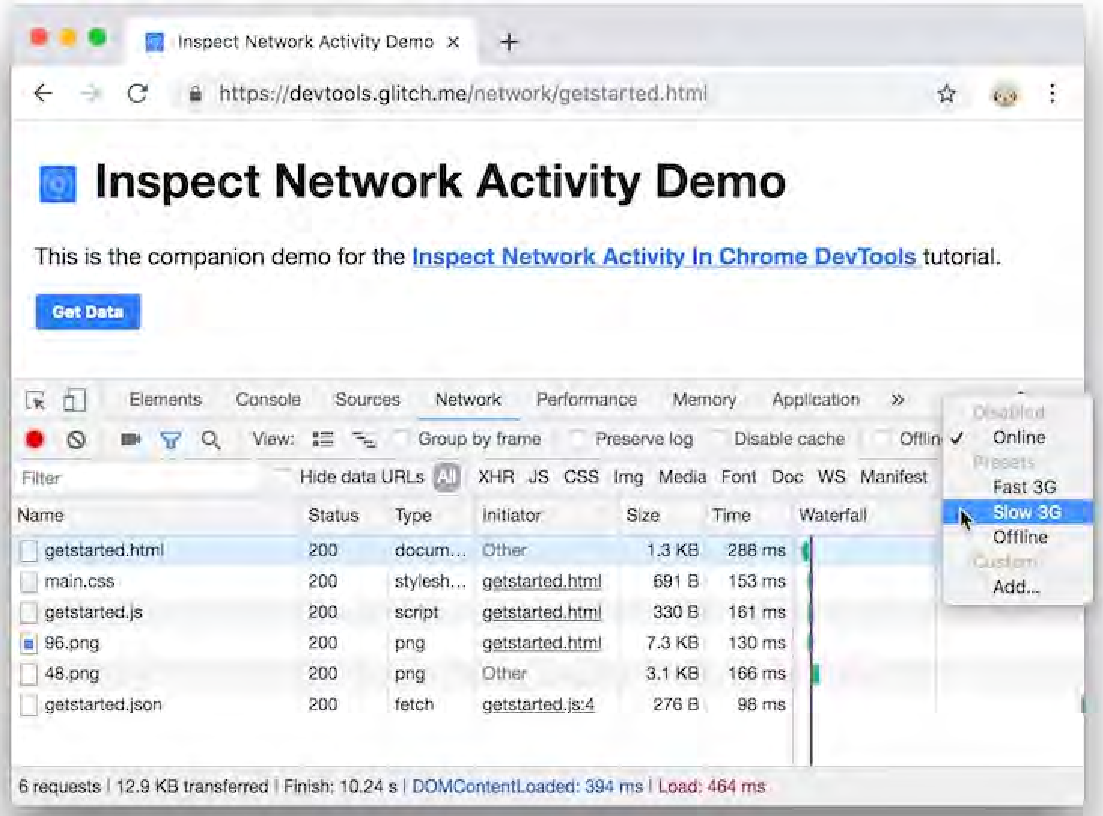
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	146 ms	
main.css	200	stylesheet	getstarted.html	691 B	109 ms	
getstarted.js	200	script	getstarted.html	330 B	124 ms	
96.png	200	png	getstarted.html	7.3 KB	10 ms	
48.png	200	png	Other	3.1 KB	7 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	88 ms	

6 requests | 12.9 KB transferred | Finish: 6.05 s | DOMContentLoaded: 244 ms | Load: 286 ms

Figure 9. Enabling throttling

2 Select **Slow 3G**.



https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

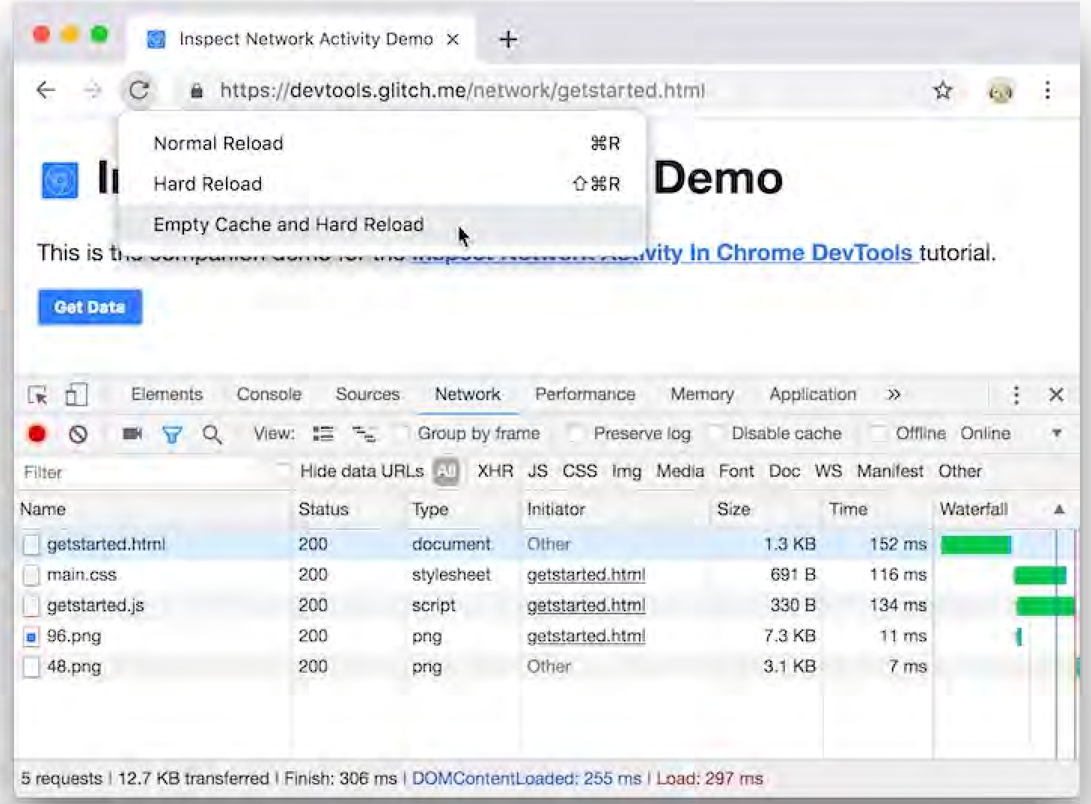
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum...	Other	1.3 KB	288 ms	
main.css	200	stylesh...	getstarted.html	691 B	153 ms	
getstarted.js	200	script	getstarted.html	330 B	161 ms	
96.png	200	png	getstarted.html	7.3 KB	130 ms	
48.png	200	png	Other	3.1 KB	166 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	98 ms	

6 requests | 12.9 KB transferred | Finish: 10.24 s | DOMContentLoaded: 394 ms | Load: 464 ms

Figure 10. Selecting Slow 3G

3 Long-press **Reload** ↻ and then select **Empty Cache And Hard Reload**.



Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	152 ms	
main.css	200	stylesheet	getstarted.html	691 B	116 ms	
getstarted.js	200	script	getstarted.html	330 B	134 ms	
96.png	200	png	getstarted.html	7.3 KB	11 ms	
48.png	200	png	Other	3.1 KB	7 ms	

5 requests | 12.7 KB transferred | Finish: 306 ms | DOMContentLoaded: 255 ms | Load: 297 ms

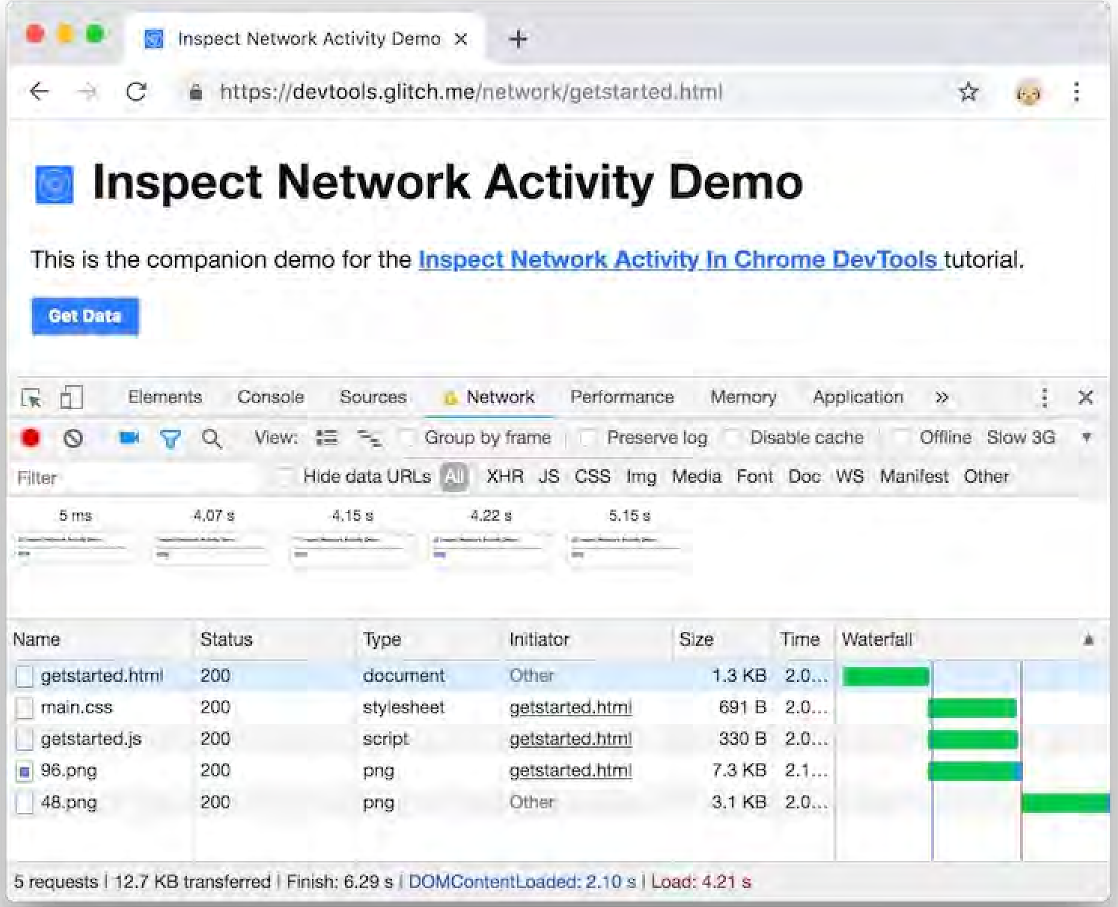
Figure 11. Empty Cache And Hard Reload

On repeat visits, the browser usually serves some files from its cache, which speeds up the page load. **Empty Cache And Hard Reload** forces the browser to go the network for all resources. This is helpful when you want to see how a first-time visitor experiences a page load.

> **Note** The **Empty Cache And Hard Reload** workflow is only available when DevTools is open.

Capture screenshots

2 Reload the page again via the **Empty Cache And Hard Reload** workflow. See [Simulate a slower connection]() if you need a reminder on how to do this. The Screenshots pane provides thumbnails of how the page looked at various points during the loading process.



Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html
Elements Console Sources Network Performance Memory Application »
View: Group by frame Preserve log Disable cache Offline Slow 3G
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
5 ms 4.07 s 4.15 s 4.22 s 5.15 s

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

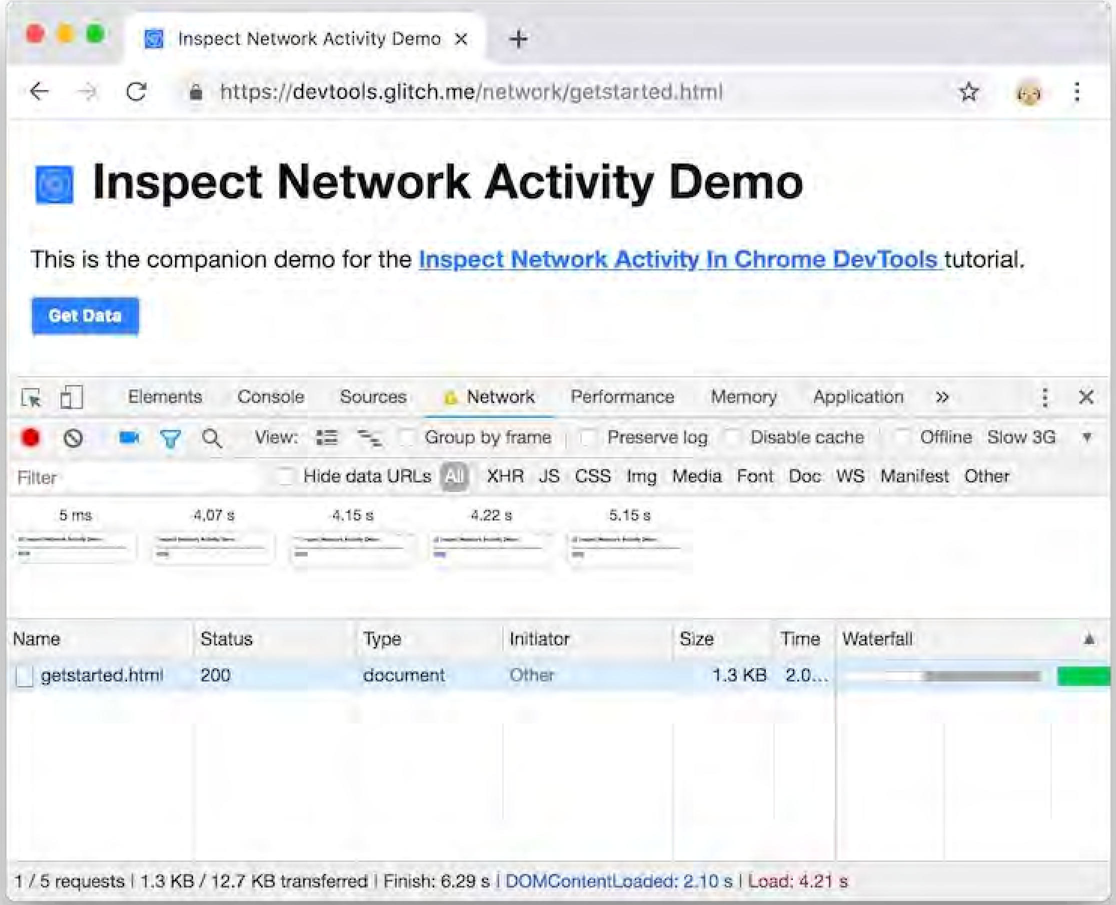
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	2.0…	
main.css	200	stylesheet	getstarted.html	691 B	2.0…	
getstarted.js	200	script	getstarted.html	330 B	2.0…	
96.png	200	png	getstarted.html	7.3 KB	2.1…	
48.png	200	png	Other	3.1 KB	2.0…	

5 requests | 12.7 KB transferred | Finish: 6.29 s | DOMContentLoaded: 2.10 s | Load: 4.21 s

Figure 12. Screenshots of the page load

3 Click the first thumbnail. DevTools shows you what network activity was occurring at that moment in time.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time
getstarted.html	200	document	Other	1.3 KB	2.0...

1 / 5 requests | 1.3 KB / 12.7 KB transferred | Finish: 6.29 s | DOMContentLoaded: 2.10 s | Load: 4.21 s

Figure 13. The network activity that was happening during the first screenshot

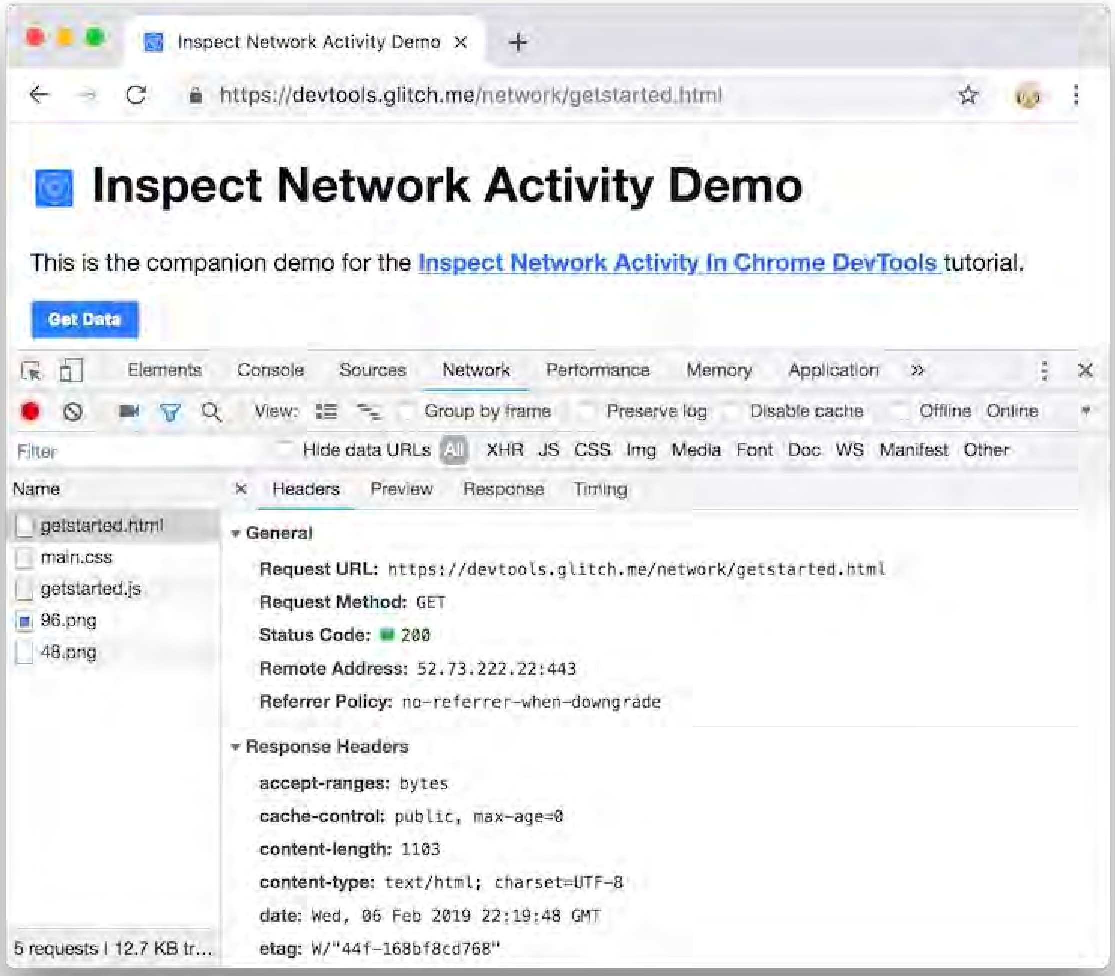
4 Click **Capture Screenshots** again to close the Screenshots pane.

5 Reload the page again.

Inspect a resource's details

Click a resource to learn more information about it. Try it now:

1 Click `getstarted.html`. The **Headers** tab is shown. Use this tab to inspect HTTP headers.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

▾ General

Request URL: `https://devtools.glitch.me/network/getstarted.html`

Request Method: GET

Status Code: 🟩 200

Remote Address: 52.73.222.22:443

Referrer Policy: no-referrer-when-downgrade

▾ Response Headers

accept-ranges: bytes

cache-control: public, max-age=0

content-length: 1103

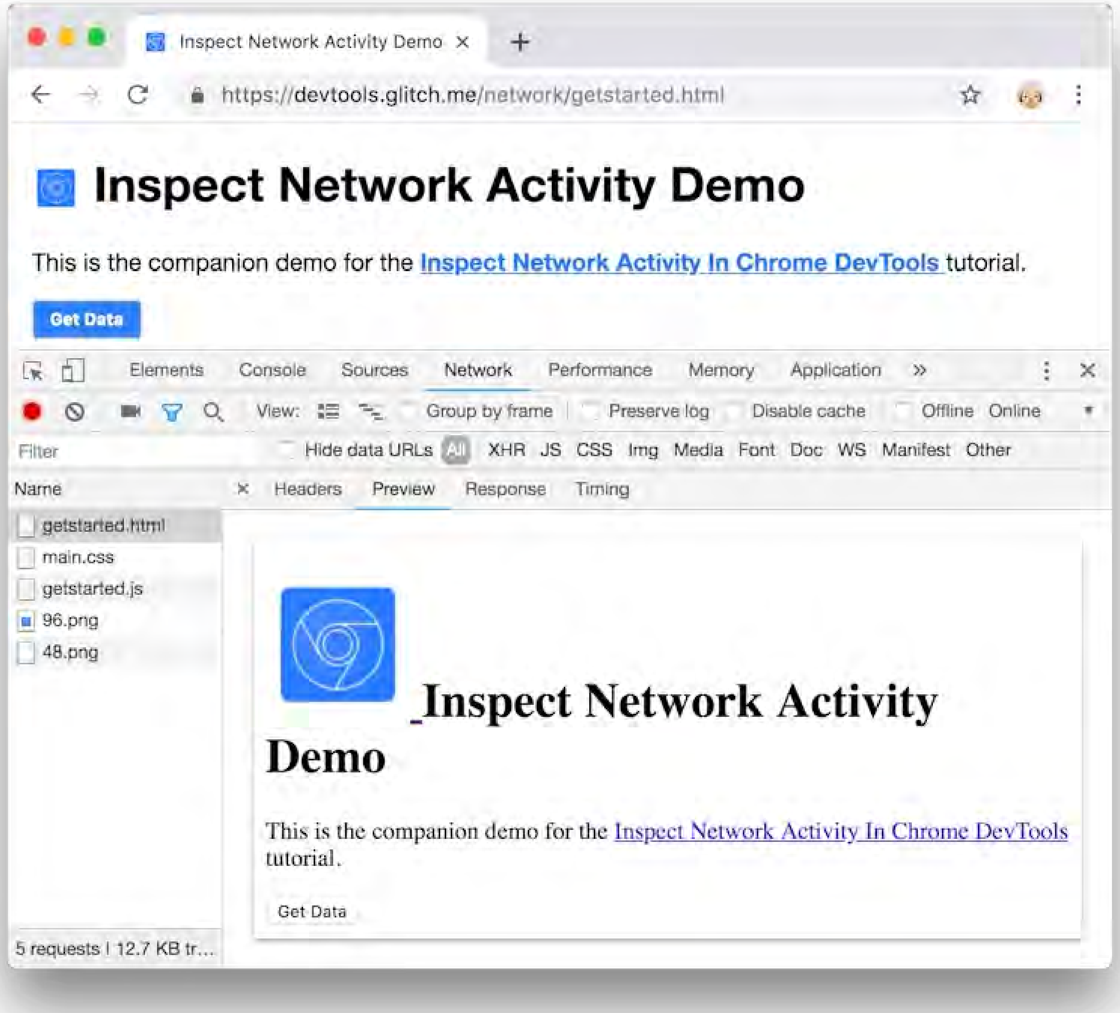
content-type: text/html; charset=UTF-8

date: Wed, 06 Feb 2019 22:19:48 GMT

etag: W/"44f-168bf8cd768"

Figure 14. The Headers tab

2 Click the **Preview** tab. A basic rendering of the HTML is shown.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

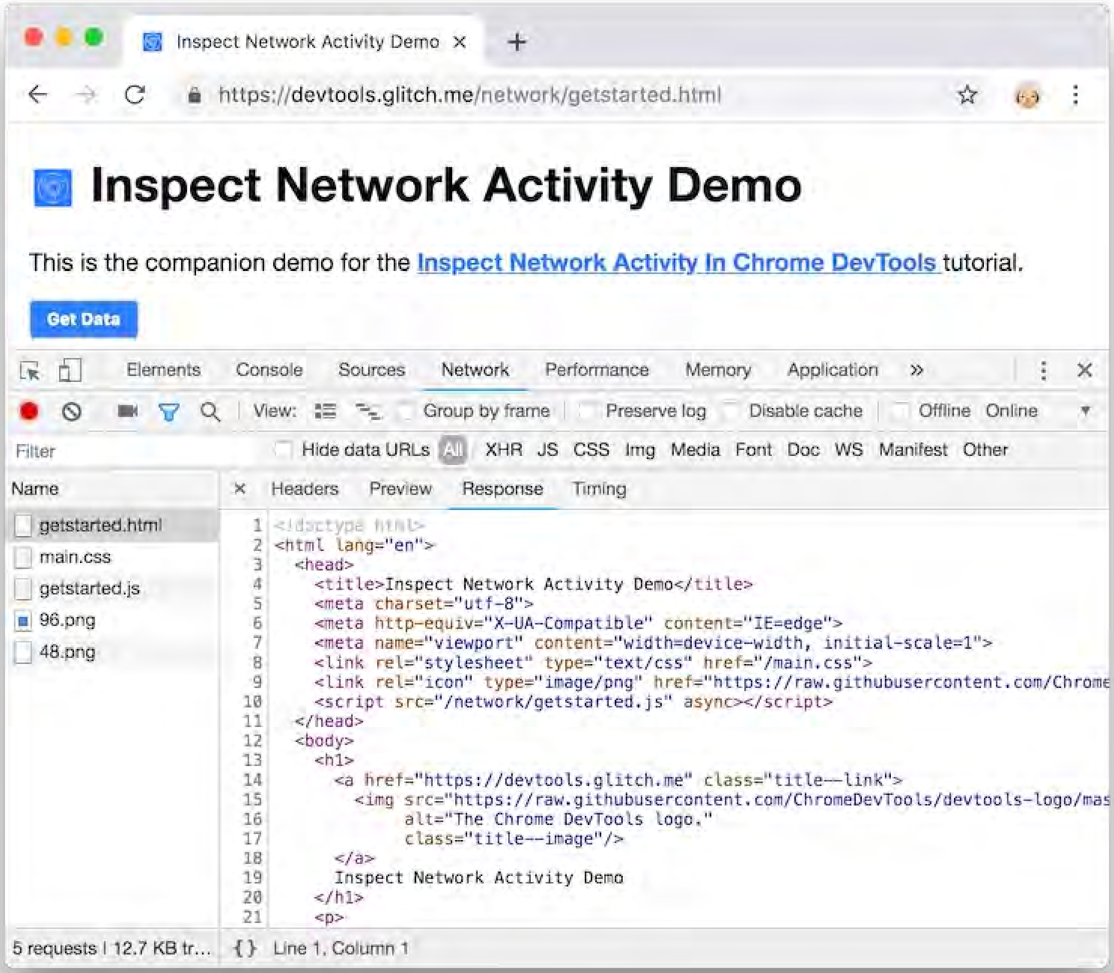
Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Figure 15. The Preview tab

This tab is helpful when an API returns an error code in HTML and it's easier to read the rendered HTML than the HTML source code, or when inspecting images.

3 Click the **Response** tab. The HTML source code is shown.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

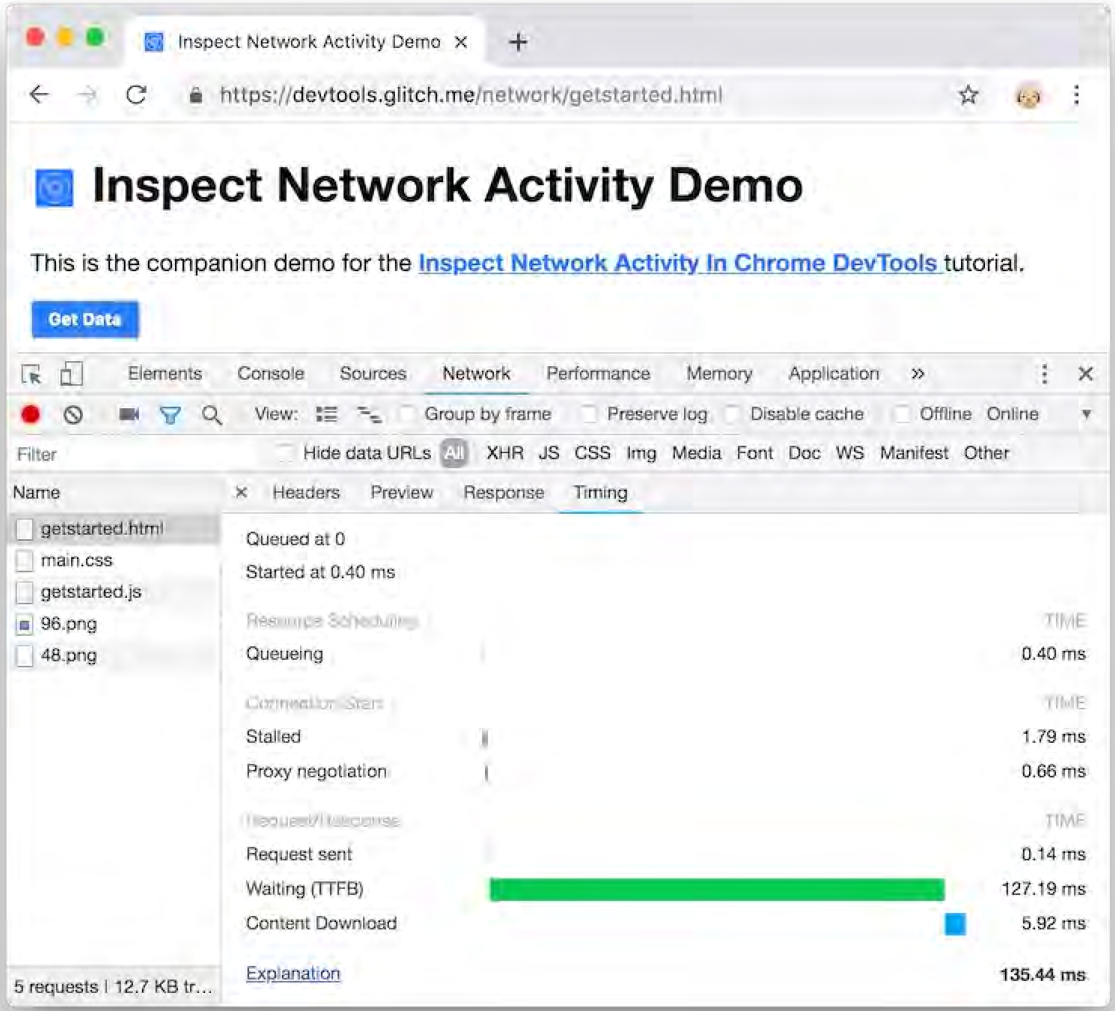
Get Data

```
<!doctype html>
<html lang="en">
  <head>
    <title>Inspect Network Activity Demo</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" href="/main.css">
    <link rel="icon" type="image/png" href="https://raw.githubusercontent.com/Chrome
    <script src="/network/getstarted.js" async></script>
  </head>
  <body>
    <h1>
      <a href="https://devtools.glitch.me" class="title--link">
        <img src="https://raw.githubusercontent.com/ChromeDevTools/devtools-logo/mas
             alt="The Chrome DevTools logo."
             class="title--image"/>
      </a>
      Inspect Network Activity Demo
    </h1>
    <p>
```

Figure 16. The Response tab

Tip When a file is minified, clicking the **Format** { } button at the bottom of the **Response** tab re-formats the file's contents for readability.

4 Click the **Timing** tab. A breakdown of the network activity for this resource is shown.



Inspect Network Activity Demo

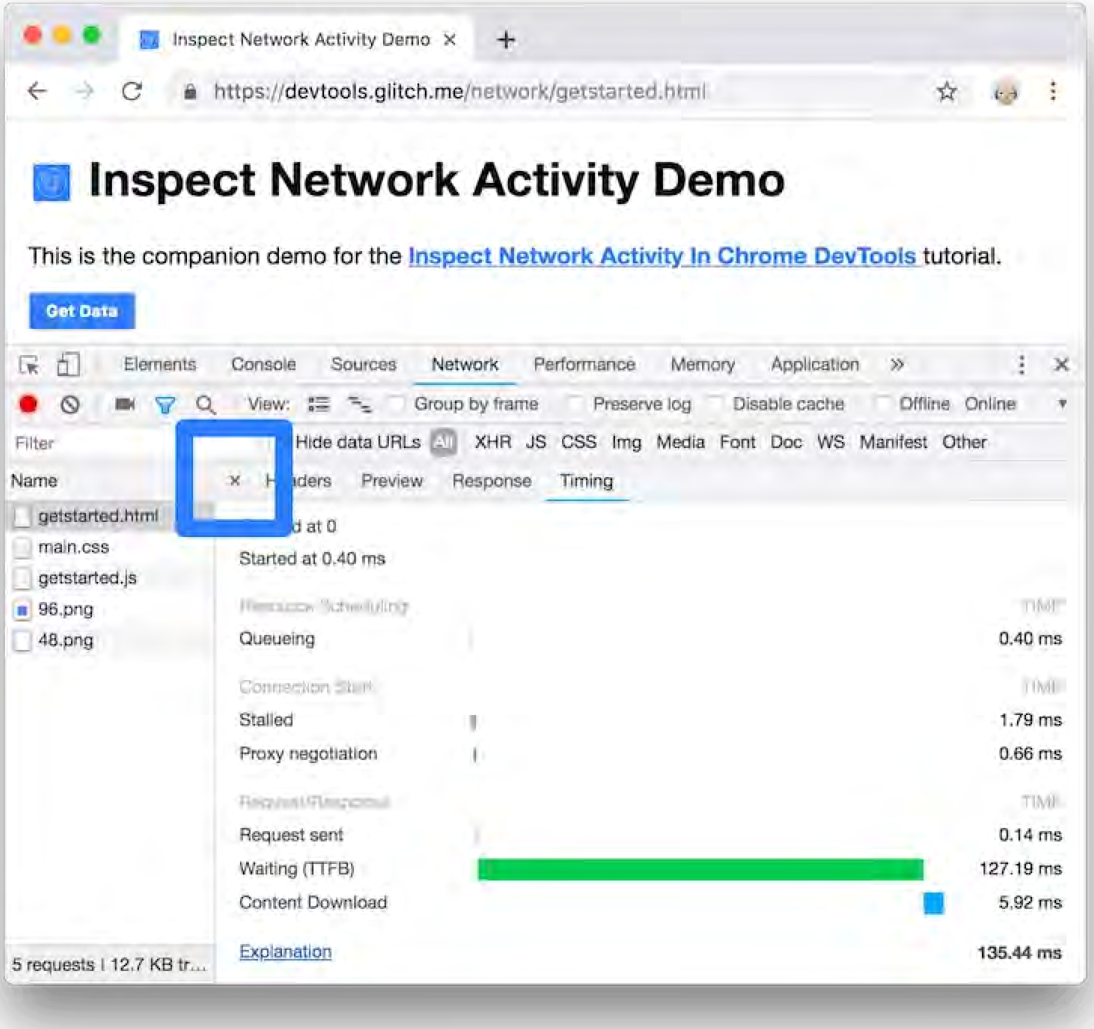
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Queued at 0
Started at 0.40 ms

Resource Scheduling	TIME
Queueing	0.40 ms
Connection Start	**TIME**
Stalled	1.79 ms
Proxy negotiation	0.66 ms
Request/Response	**TIME**
Request sent	0.14 ms
Waiting (TTFB)	127.19 ms
Content Download	5.92 ms
Explanation	135.44 ms

Figure 17. The Timing tab

5 Click **Close** ✕ to view the Network Log again.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Queued at 0
Started at 0.40 ms

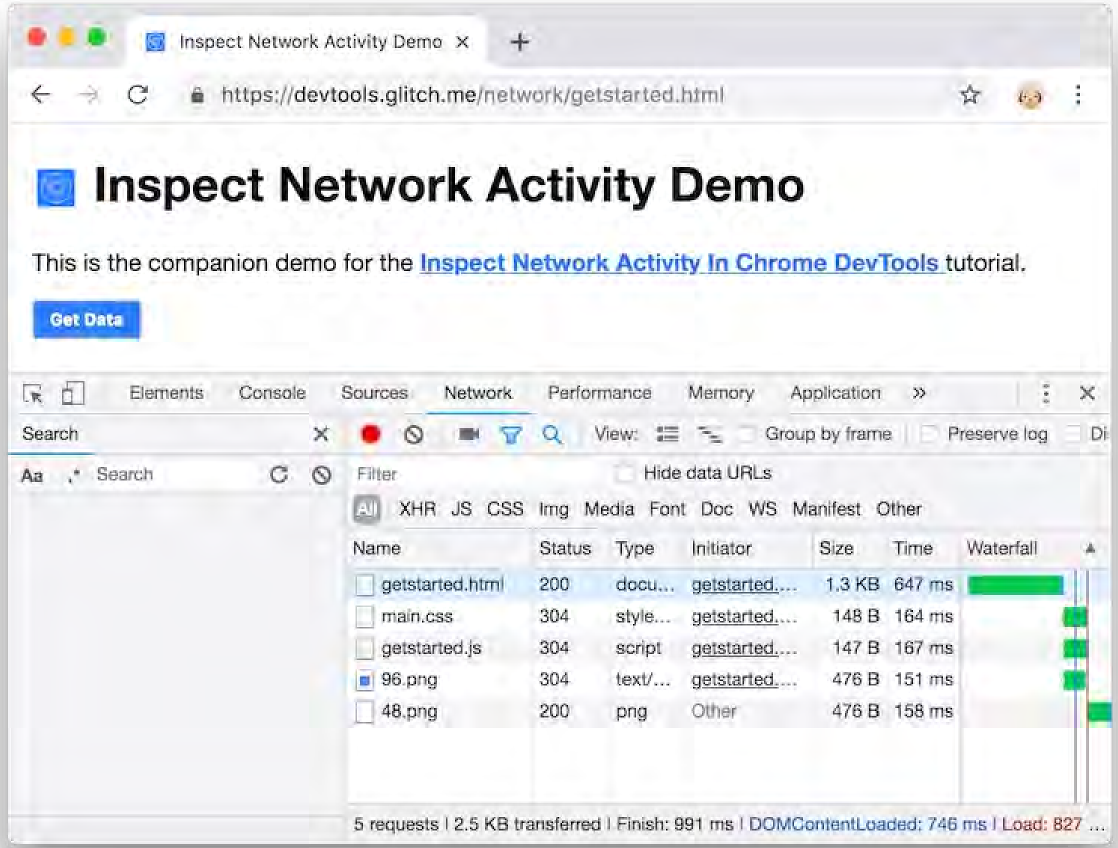
Resource Scheduling	TIME
Queueing	0.40 ms
Connection Start	TIME
Stalled	1.79 ms
Proxy negotiation	0.66 ms
Request/Response	TIME
Request sent	0.14 ms
Waiting (TTFB)	127.19 ms
Content Download	5.92 ms
Explanation	135.44 ms

Figure 18. The Close button

Search network headers and responses

Use the **Search** pane when you need to search the HTTP headers and responses of all resources for a certain string or regular expression.

For example, suppose you want to check if your resources are using reasonable cache policies.



Inspect Network Activity Demo

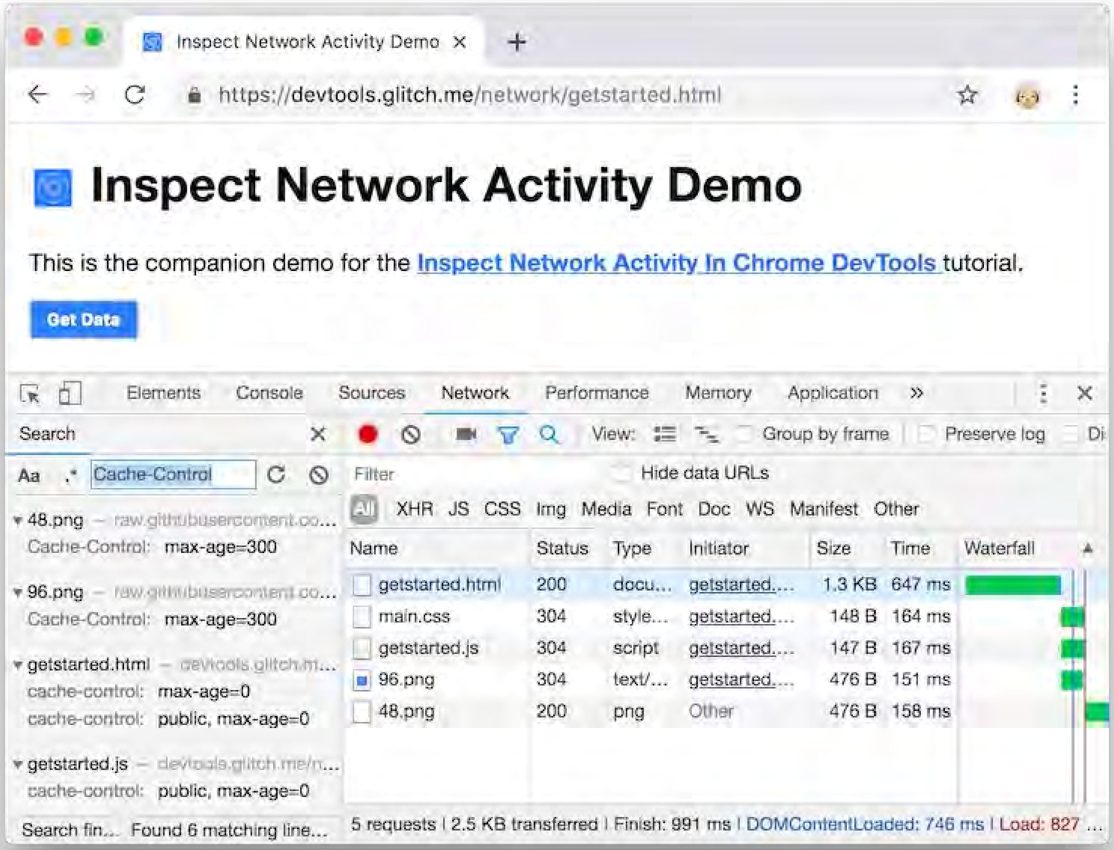
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docu...	getstarted....	1.3 KB	647 ms	
main.css	304	style...	getstarted....	148 B	164 ms	
getstarted.js	304	script	getstarted....	147 B	167 ms	
96.png	304	text/...	getstarted....	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ...

Figure 19. The Search pane

2 Type `Cache-Control` and press Enter. The Search pane lists all instances of `Cache-Control` that it finds in resource headers or content.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Cache-Control

▾ 48.png — raw.githubusercontent.co...
Cache-Control: max-age=300

▾ 96.png — raw.githubusercontent.co...
Cache-Control: max-age=300

▾ getstarted.html — devtools.glitch.m...
cache-control: max-age=0
cache-control: public, max-age=0

▾ getstarted.js — devtools.glitch.me/n...
cache-control: public, max-age=0

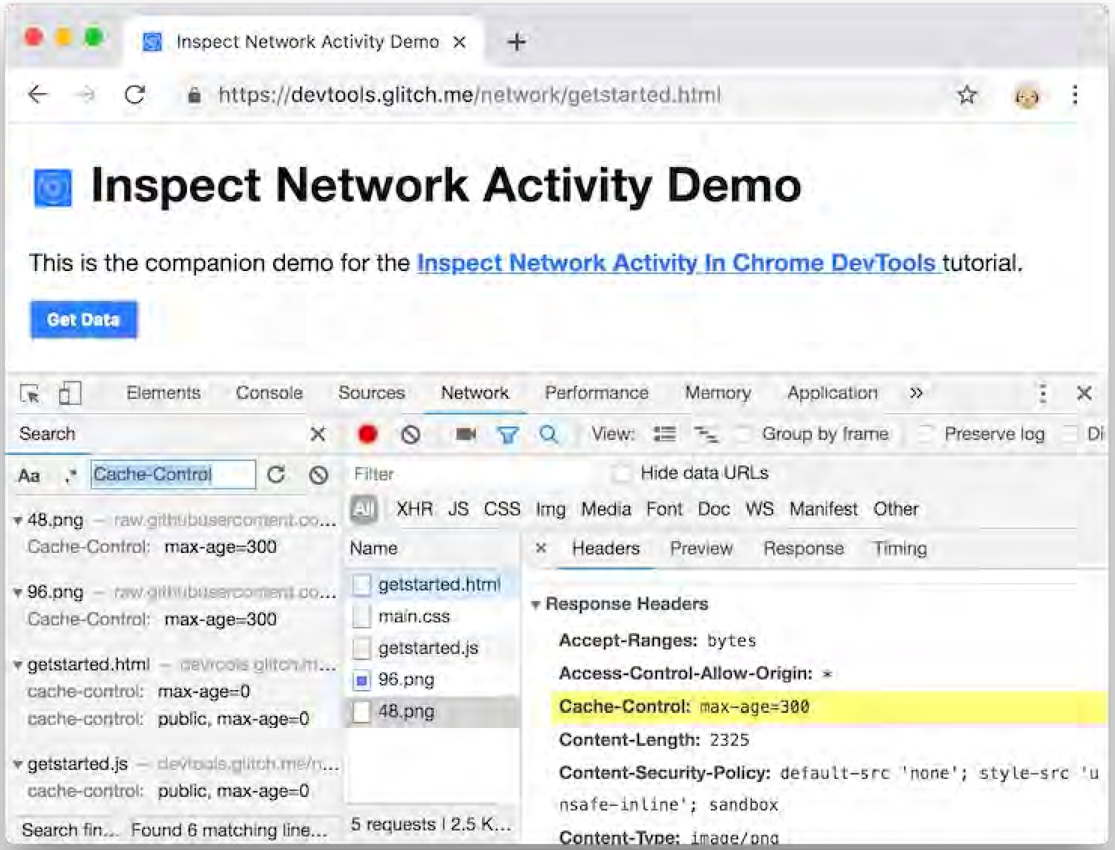
Search fin... Found 6 matching line...

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docu...	getstarted....	1.3 KB	647 ms	
main.css	304	style...	getstarted....	148 B	164 ms	
getstarted.js	304	script	getstarted....	147 B	167 ms	
96.png	304	text/...	getstarted....	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ...

Figure 20. Search results for `Cache-Control`

3 Click a result to view it. If the query was found in a header, the Headers tab opens. If the query was found in content, the Response tab opens.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

48.png — raw.githubusercontent.co...
Cache-Control: max-age=300

96.png — raw.githubusercontent.co...
Cache-Control: max-age=300

getstarted.html — devtools.glitch.m...
cache-control: max-age=0
cache-control: public, max-age=0

getstarted.js — devtools.glitch.me/n...
cache-control: public, max-age=0

Search fin... Found 6 matching line...

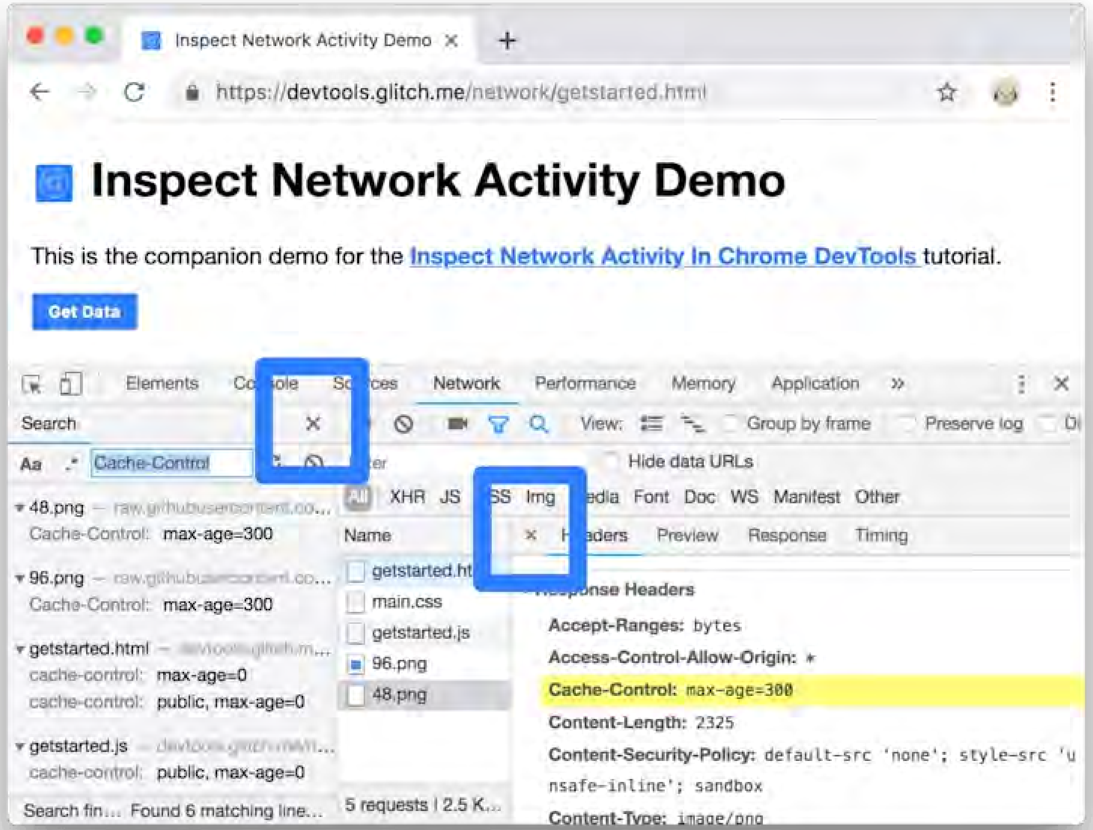
getstarted.html
main.css
getstarted.js
96.png
48.png

5 requests | 2.5 K...

Response Headers
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: max-age=300
Content-Length: 2325
Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox
Content-Type: image/png

Figure 21. A search result highlighted in the Headers tab

4 Close the Search pane and the Timing tab.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Aa .* Cache-Control

- 48.png — raw.githubusercontent.co...
  Cache-Control: max-age=300
- 96.png — raw.githubusercontent.co...
  Cache-Control: max-age=300
- getstarted.html — devtools.glitch.m...
  cache-control: max-age=0
  cache-control: public, max-age=0
- getstarted.js — devtools.glitch.m...
  cache-control: public, max-age=0

Search fin... Found 6 matching line...

getstarted.html
main.css
getstarted.js
96.png
48.png

5 requests | 2.5 K...

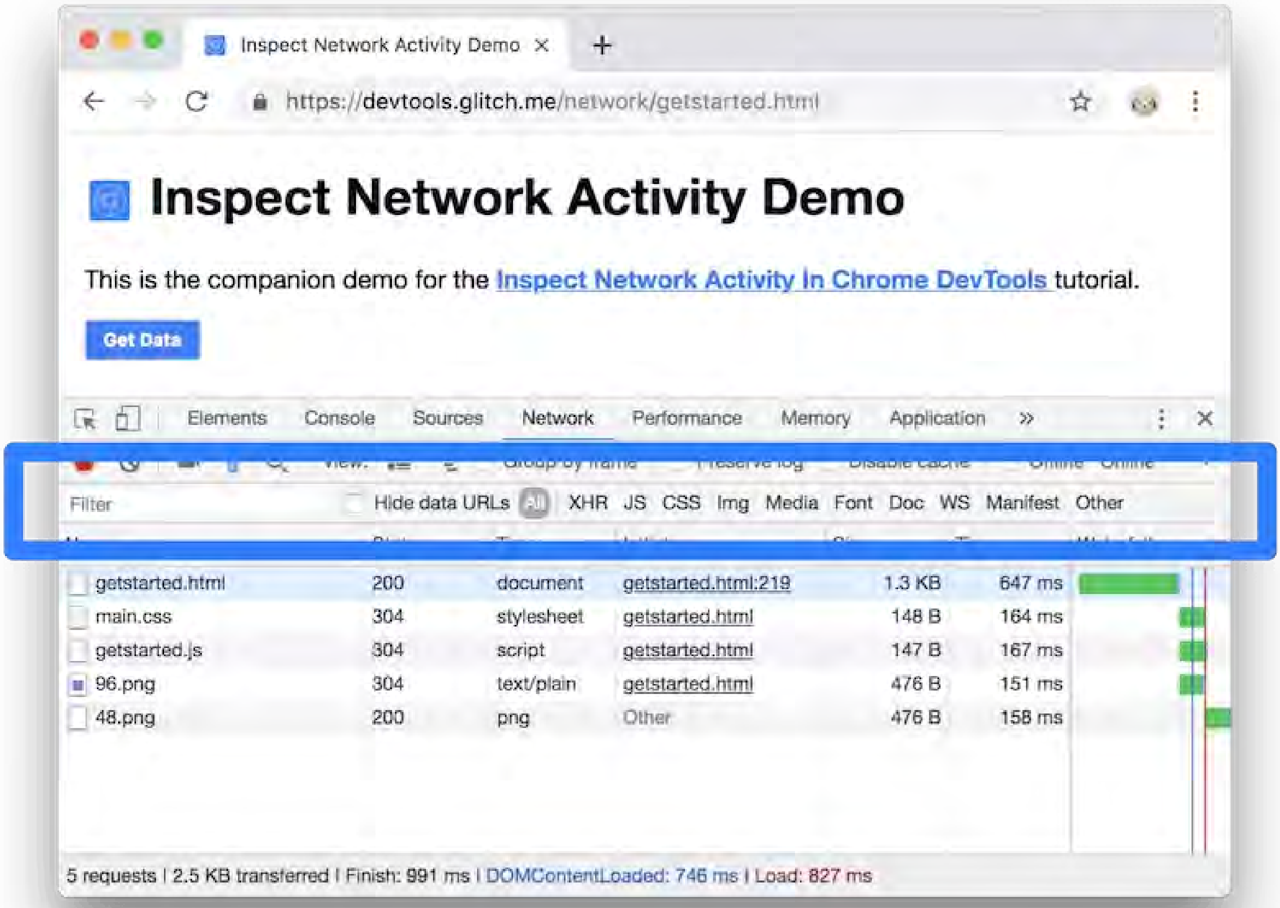
Response Headers

```
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: max-age=300
Content-Length: 2325
Content-Security-Policy: default-src 'none'; style-src 'u
nsafe-inline'; sandbox
Content-Type: image/png
```

Figure 22. The Close buttons

Filter resources

DevTools provides numerous workflows for filtering out resources that aren't relevant to the task at hand.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

getstarted.html	200	document	getstarted.html:219	1.3 KB	647 ms
main.css	304	stylesheet	getstarted.html	148 B	164 ms
getstarted.js	304	script	getstarted.html	147 B	167 ms
96.png	304	text/plain	getstarted.html	476 B	151 ms
48.png	200	png	Other	476 B	158 ms

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

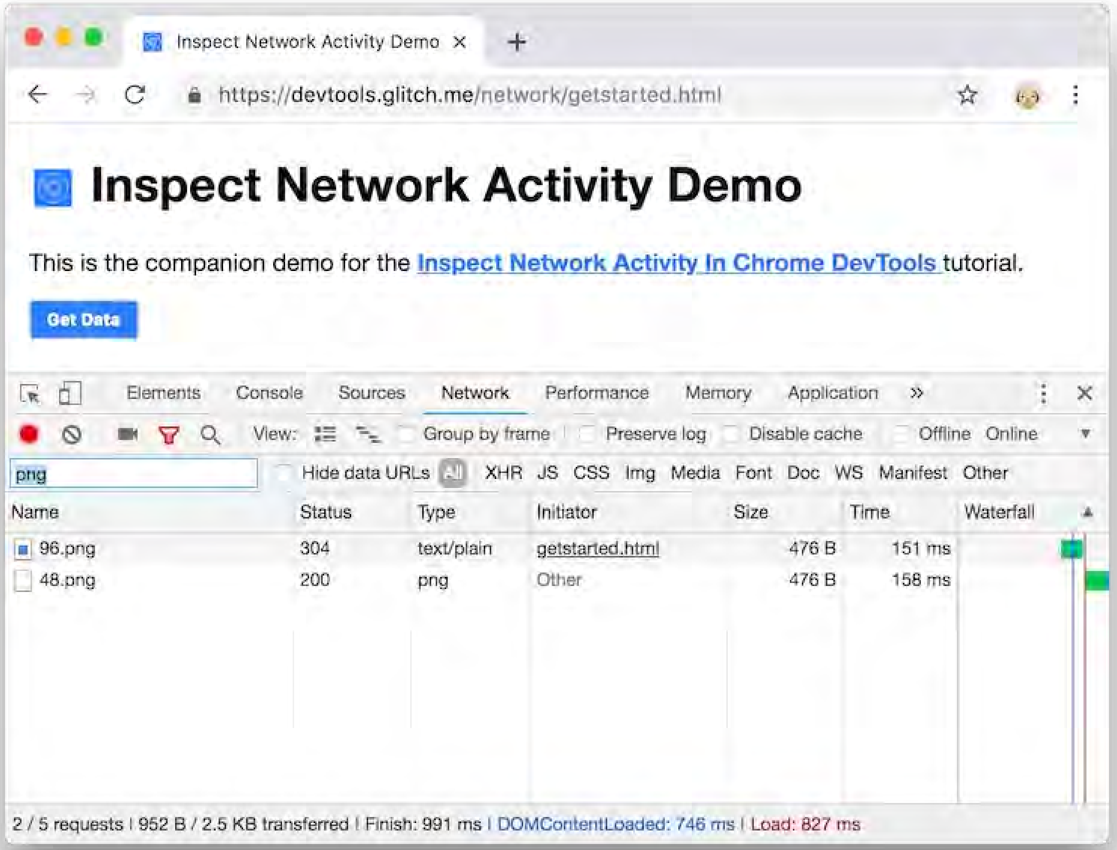
Figure 23. The Filters toolbar

The **Filters** toolbar should be enabled by default. If not:

1 Click **Filter** ▽ to show it.

Filter by string, regular expression, or property

The **Filter** text box supports many different types of filtering.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

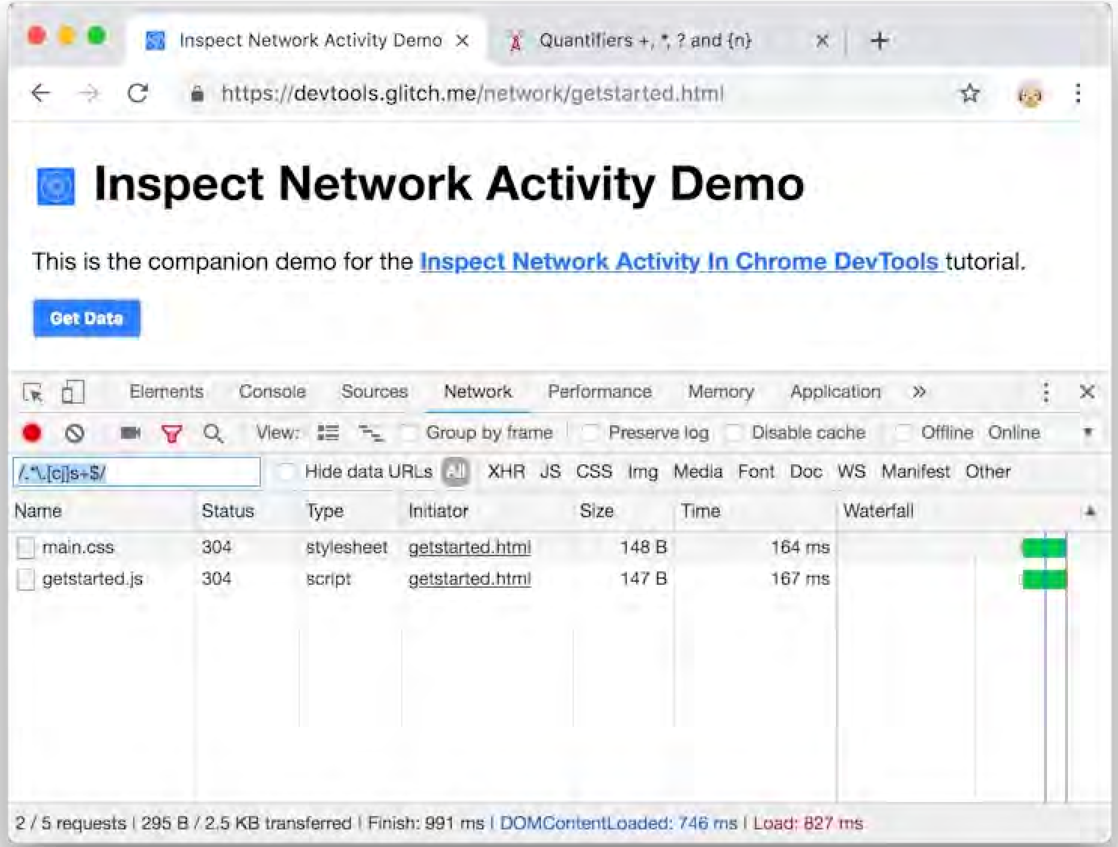
png

Name	Status	Type	Initiator	Size	Time	Waterfall
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

2 / 5 requests | 952 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 24. A string filter

2 Type `/.*\.[cj]s+$/`. DevTools filters out any resource with a filename that doesn't end with a `j` or a `c` followed by 1 or more `s` characters.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

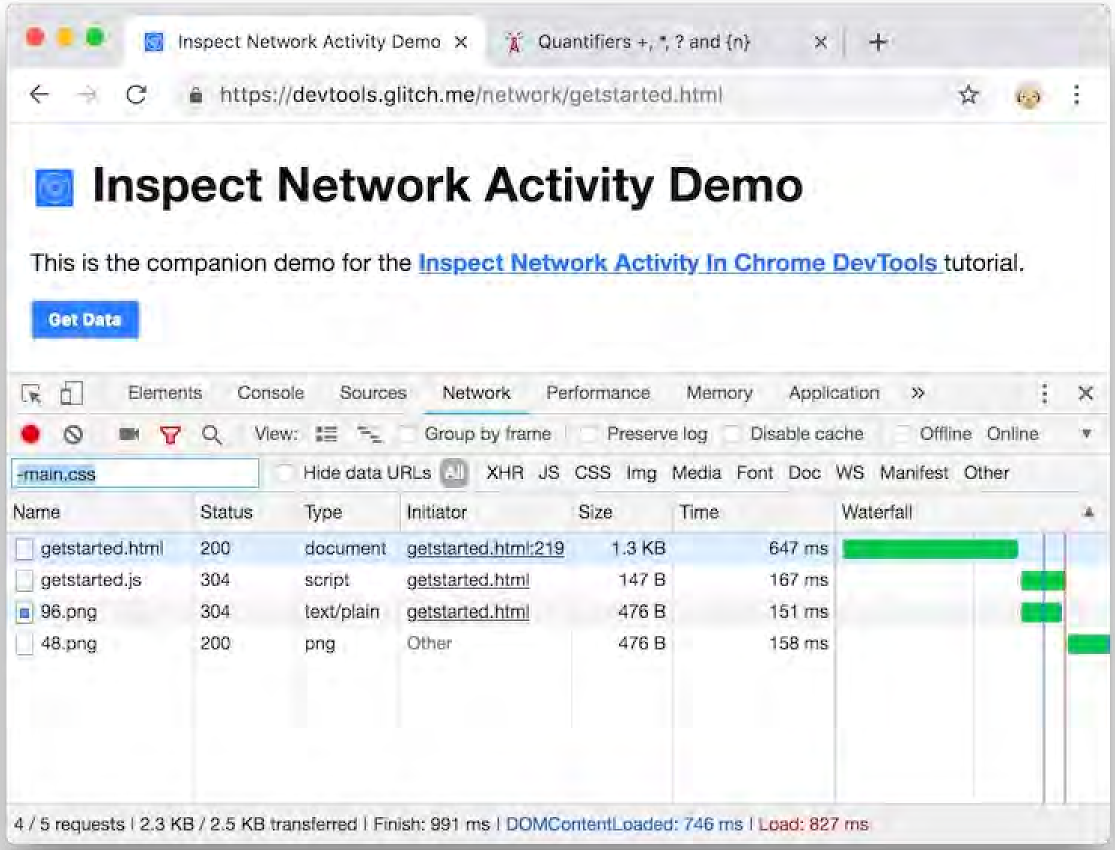
/.*\.[cj]s+$/

Name	Status	Type	Initiator	Size	Time	Waterfall
main.css	304	stylesheet	getstarted.html	148 B	164 ms	
getstarted.js	304	script	getstarted.html	147 B	167 ms	

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 25. A regular expression filter

3 Type `-main.css`. DevTools filters out `main.css`. If any other file matched the pattern they would also be filtered out.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

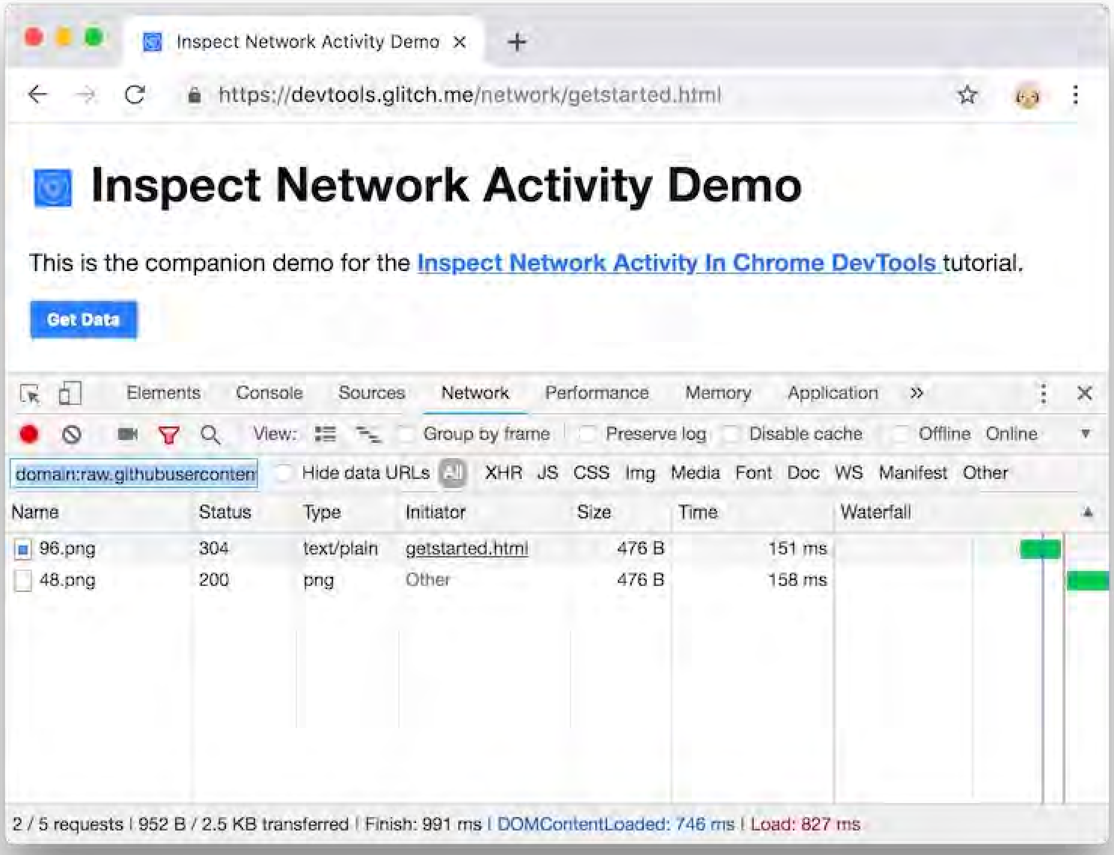
-main.css

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	getstarted.html:219	1.3 KB	647 ms	
getstarted.js	304	script	getstarted.html	147 B	167 ms	
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

4 / 5 requests | 2.3 KB / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 26. A negative filter

4 Type `domain:raw.githubusercontent.com` into the **Filter** text box. DevTools filters out any resource with a URL that does not match this domain.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

domain:raw.githubusercontent

Name	Status	Type	Initiator	Size	Time	Waterfall
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

2 / 5 requests | 952 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 27. A property filter

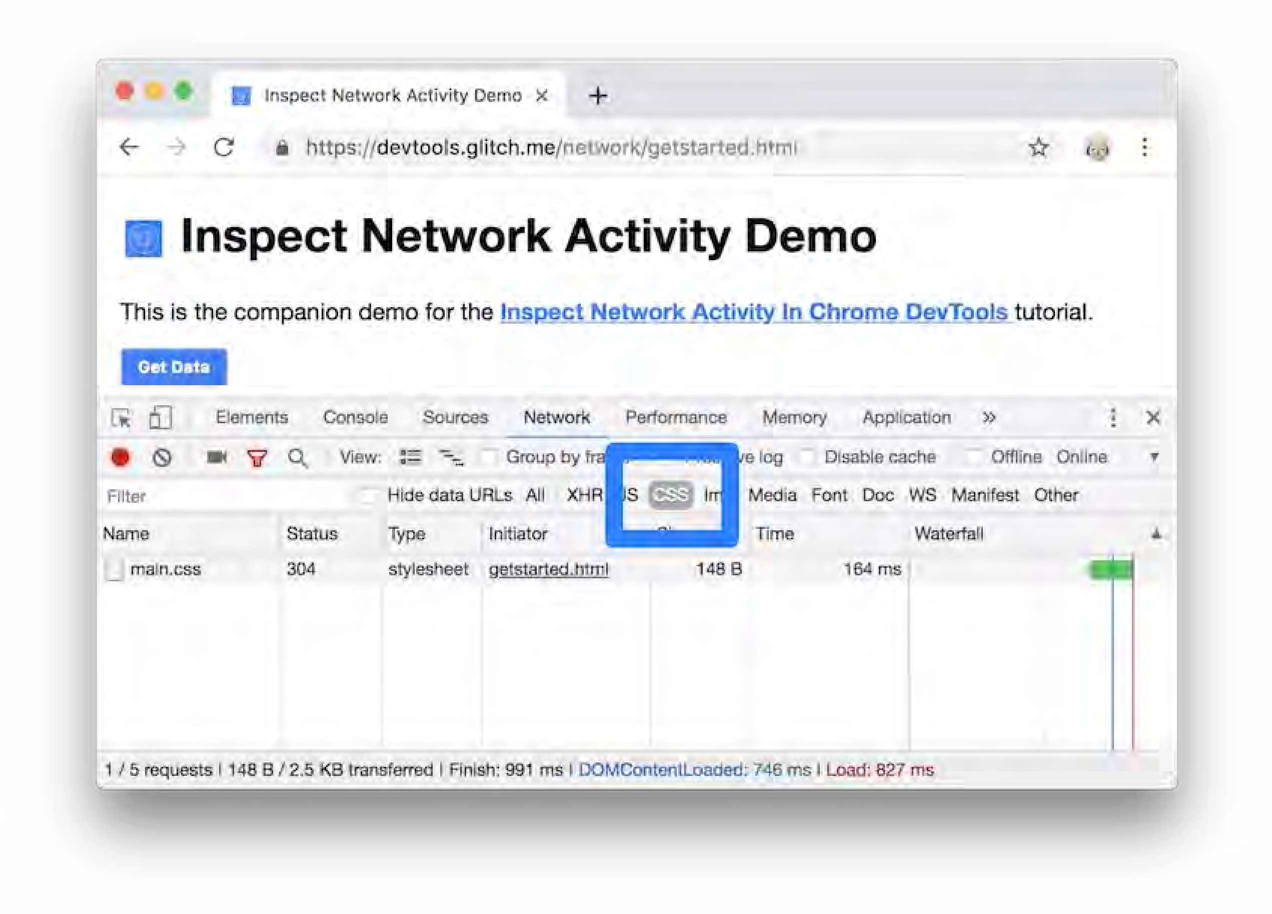
See Filter requests by properties for the full list of filterable properties.

5 Clear the **Filter** text box of any text.

Filter by resource type

To focus in on a certain type of file, such as stylesheets:

1 Click **CSS**. All other file types are filtered out.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

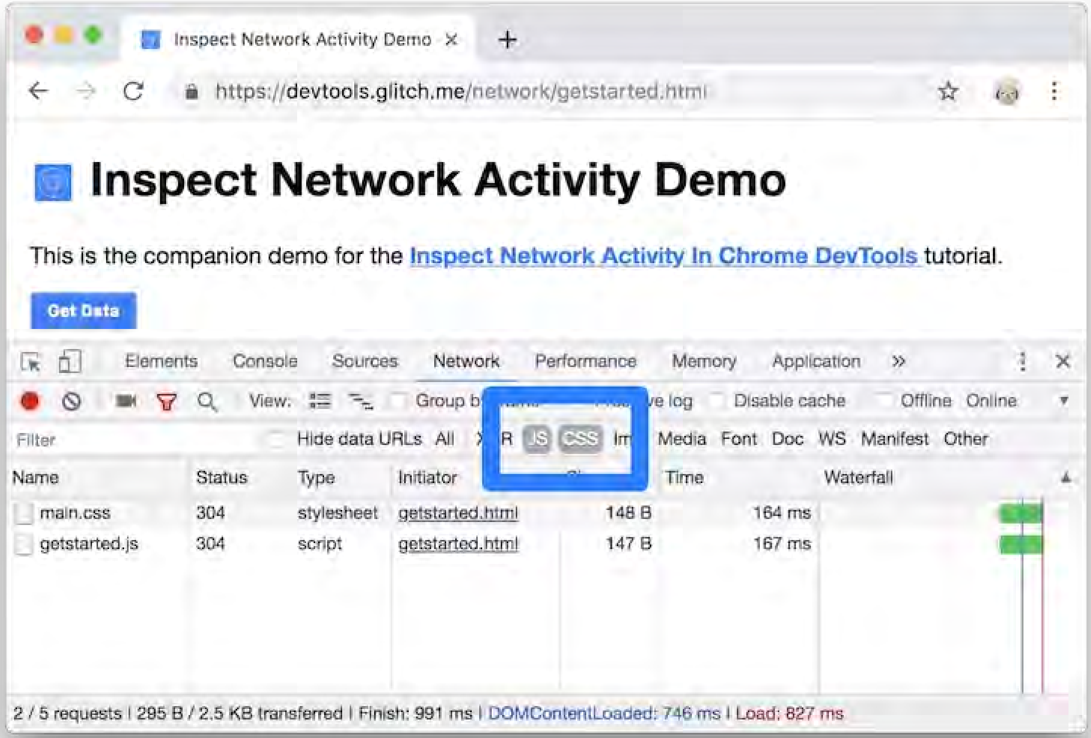
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
main.css	304	stylesheet	getstarted.html	148 B	164 ms	

1 / 5 requests | 148 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 28. Showing CSS files only

2 To also see scripts, hold Control or Command (Mac) and then click **JS**.



This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator		Time	Waterfall
main.css	304	stylesheet	getstarted.html	148 B	164 ms	
getstarted.js	304	script	getstarted.html	147 B	167 ms	

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 29. Showing CSS and JS files only

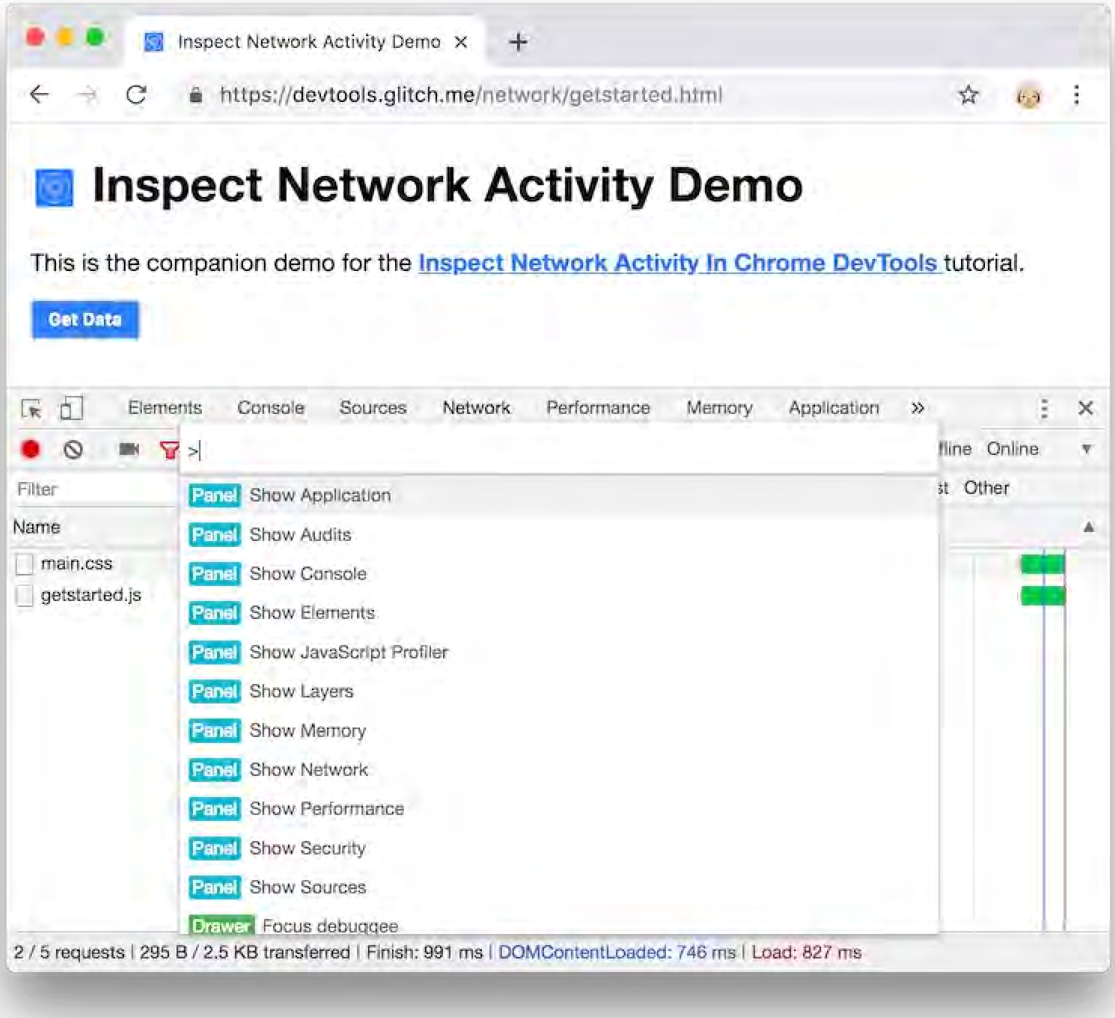
3 Click **All** to remove the filters and see all resources again.

See Filter requests for other filtering workflows.

Block requests

How does a page look and behave when some of its resources aren't available? Does it fail completely, or is it still somewhat functional? Block requests to find out:

1 Press Control+Shift+P or Command+Shift+P (Mac) to open the **Command Menu**.



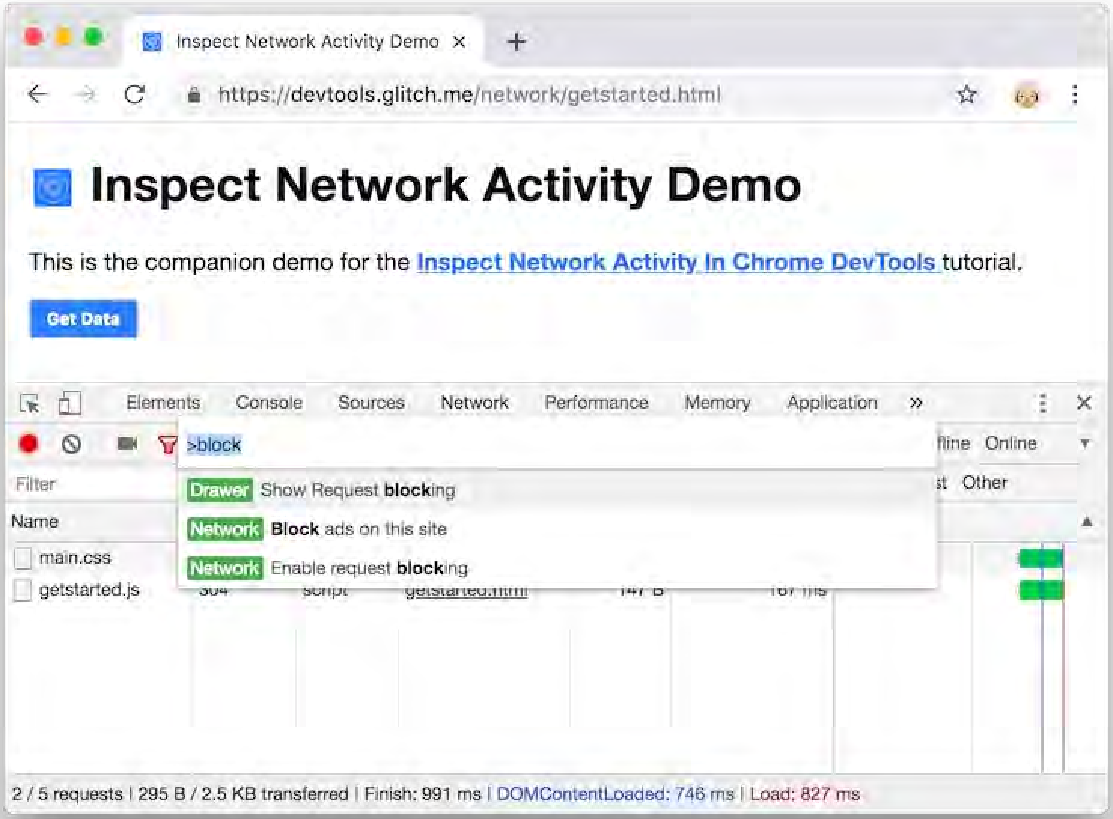
Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 30. The Command Menu

2 Type `block`, select **Show Request Blocking**, and press Enter.



Inspect Network Activity Demo

https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

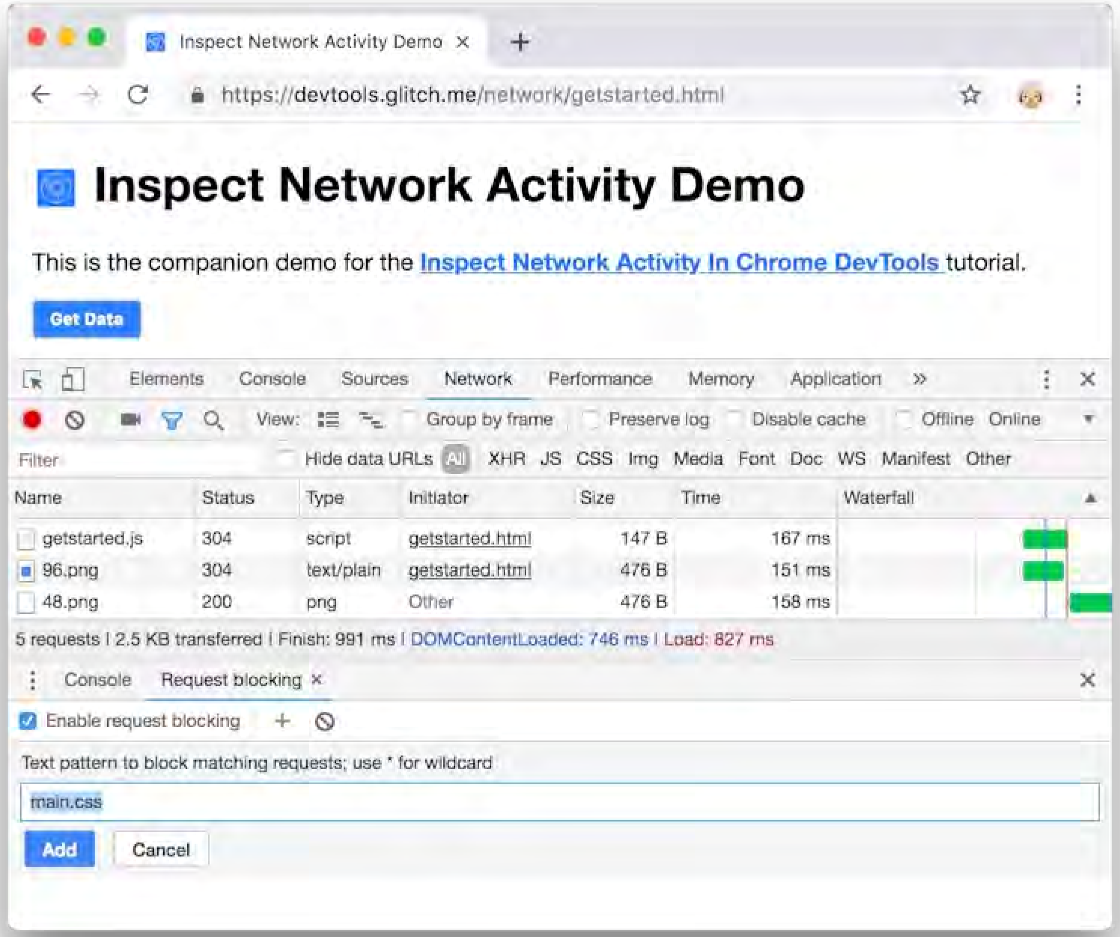
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 31. Show Request Blocking

3 Click **Add Pattern** +.

4 Type `main.css`.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.js	304	script	getstarted.html	147 B	167 ms	
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

☑ Enable request blocking

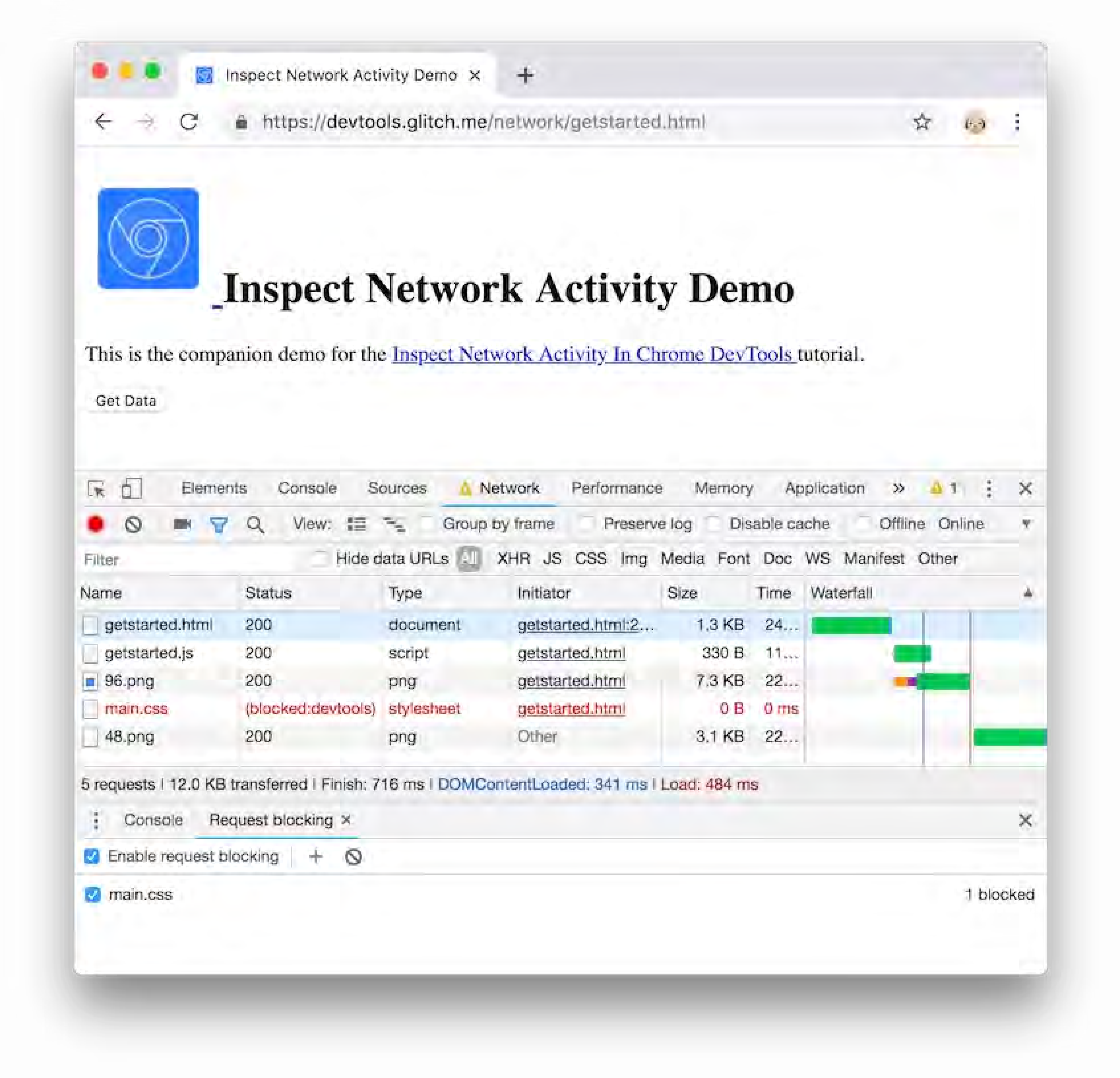
Text pattern to block matching requests; use * for wildcard

main.css

Figure 32. Blocking `main.css`

5 Click **Add**.

6 Reload the page. As expected, the page's styling is slightly messed up because its main stylesheet has been blocked. Note the `main.css` row in the Network Log. The red text means that the resource was blocked.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time
getstarted.html	200	document	getstarted.html:2...	1.3 KB	24...
getstarted.js	200	script	getstarted.html	330 B	11...
96.png	200	png	getstarted.html	7.3 KB	22...
main.css	(blocked:devtools)	stylesheet	getstarted.html	0 B	0 ms
48.png	200	png	Other	3.1 KB	22...

5 requests | 12.0 KB transferred | Finish: 716 ms | DOMContentLoaded: 341 ms | Load: 484 ms

☑ Enable request blocking

☑ main.css 1 blocked

Figure 33. `main.css` has been blocked

7 Uncheck the **Enable request blocking** checkbox.

Next steps

Congratulations, you have completed the tutorial. Click **Dispense Award** to receive your award.

Follow us

Contribute

File a bug

View source

Related content

web.dev

Case studies

Podcasts

Connect

Twitter

YouTube

GitHub

Google for Developers

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #205

Support
moz://a

Firefox accounts will be renamed Mozilla accounts on Nov 1
You'll still sign in with the same username and password, and there are no other changes to the products that you use. You may see updated help articles that refer to Mozilla accounts before Nov 1.
Learn more

Protect your privacy

Find help...

Customize this article

Download Firefox

Systems and Languages What's New Privacy

Common Myths about Private Browsing

Private Browsing is a useful feature of Firefox, but only if you understand the protection it offers. It helps you obscure your online activity from other people who use Firefox on your computer, but does not make you invisible online.

Myth 1: Private Browsing makes you anonymous on the Internet

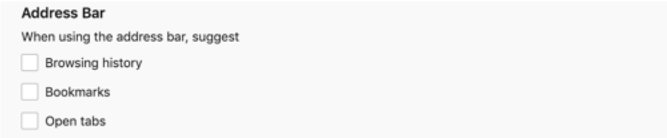
Reality: Private Browsing does not mask your identity or activity online. Websites and internet service providers can still gather information about your visit, even if you are not signed in. If you use your device at work, your company may be able to monitor the websites you visit. If you surf the Web at home, your cable company (or their partners) may have access to your browsing information. Only a Virtual Private Network (VPN) can mask your location and encrypt your online activity, keeping your identity and data safe from prying eyes. If you need to stay anonymous online, try Mozilla VPN.

Myth 2: Private Browsing removes all traces of your browsing activity from your computer

Reality: Private Browsing works by letting you browse without saving passwords, cookies and browsing history in a Private Window. If you download a file from a website, it will remain on your computer, but it will not appear in the download manager in Firefox. If you bookmark a website while in a Private Window, it will remain in your bookmark list.

Myth 3: Private Browsing doesn't display any browsing history

Reality: Private Browsing will, by default, display visited sites and bookmarks as you type in the address bar. Firefox saves these pages during normal browsing. If you don't want to see these suggestions, you can deselect them in your Firefox Settings Privacy & Security panel under *Address Bar*.


Address Bar
When using the address bar, suggest
□ Browsing history
□ Bookmarks
□ Open tabs

Myth 4: Private Browsing will protect you from keystroke loggers and spyware

Reality: Private Browsing does not protect you from malware installed on your computer. If you suspect you have malware, take steps to remove it to prevent it from happening again.

To learn more about how Firefox protects your privacy, see Enhanced Tracking Protection in Firefox for desktop and SmartBlock for Enhanced Tracking Protection.

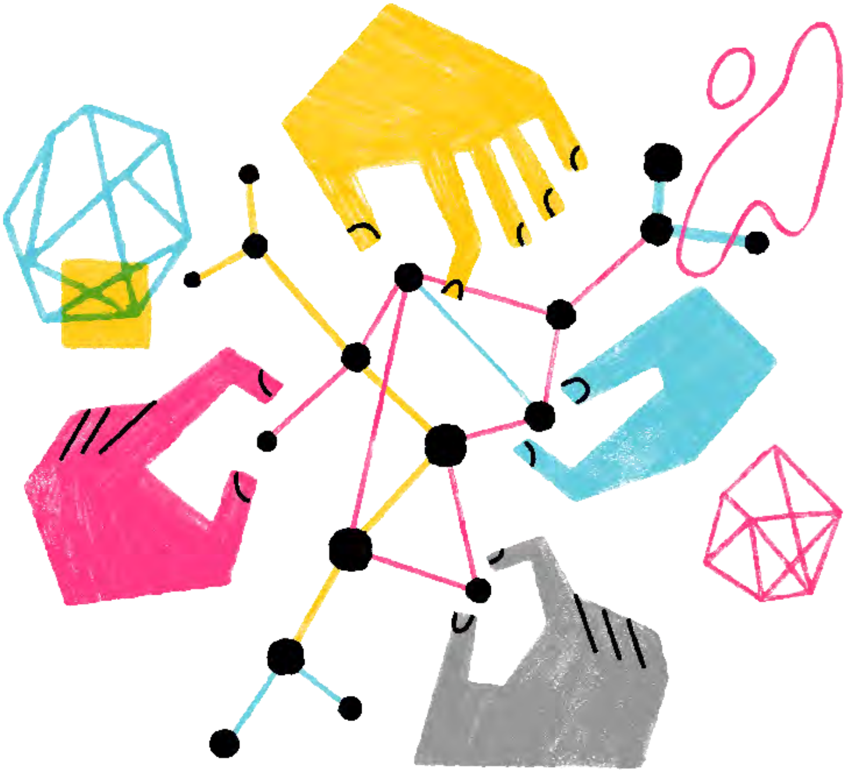
Support
moz://a

Was this article helpful?

👍 👎

These fine people helped write this article:

AliceWyman, Michele Rodaro, Mozinet, Joni, Artist, Jeff, Erin S., Fabi, k_alex, Bithiah, JeremyKoozar, alineee



Volunteer

Grow and share your expertise with others. Answer questions and improve our knowledge base.

Learn More

Mozilla	Firefox	Firefox for Developers
Report Trademark Abuse	Download	Developer Edition
Source code	Firefox Desktop	Beta

Support
moz://a

Beta for Android

Nightly

Nightly for Android

Explore Help Articles

Firefox Accounts

Sign In/Up

Benefits

Focus Browser

Language

English

Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.

mozilla.org Terms of Service Privacy Cookies Contact

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #227

- Home
- Privacy Policy
- Thank You
  - Congratulations! You told Congress to create a “Do Not Track Me” list.
- About
- Take Action
  - Privacy Toolbox
  - Sign a Petition
  - File a Complaint
- Blog
- In the News
- Press Releases
- Videos

Subscribe: Posts | Comments

Consumer Watchdog's

Inside Google

Inside Google

Search this site

- Action »
- Blog Posts
- Clout
- Discussing Search
- Don't Show on Homepage
- In the News
- Press Releases
- Privacy
- Videos
- View All

Consumer Watchdog.org

Google Chrome Privacy Issues Prompts Plea To Google Execs

Thomas Claburn

Tue, Nov 4, 2008 at 1:00 pm

Chief among the group’s complaints is Google Suggest, a feature found in Chrome and other Google applications like Google Toolbar.

In an effort to publicize what it claims are the privacy failings of Google’s new Chrome browser, Consumer Watchdog is airing its grievances through Google’s YouTube and urging viewers to use its e-mail form to submit a message to Google’s board of directors demanding better privacy protection.

Google’s new Chrome browser presents a privacy risk for consumers, the consumer advocacy group contends, because it sends information about users’ searches "without users’ full understanding, consent or control."

Google launched its open source Chrome browser, now in its third beta iteration (version 0.3.154.9), in early September to provide a better experience and better security for browser-based applications.

Chrome’s Incognito mode, like Microsoft Internet Explorer 8 Beta 2’s InPrivate mode and Apple Safari’s Private Browsing mode, creates a window in which, as Google puts it, nothing "is ever logged on your computer."

Consumer Watchdog argues that Chrome’s Incognito mode does not confer the privacy that the mode’s name suggests and that Chrome’s blurring of local and remote computing "creates confusion in the consumer’s mind about the privacy and security of confidential information."

Chief among the group’s complaints is Google Suggest, a feature found in Chrome and other Google applications like Google Toolbar. It is effectively a keystroke logger than sends every character typed to Google. Google uses this information to provide search suggestions that it refines with every subsequent letter.

Google doesn’t see the harm in this. "Just as E.T. needs to phone home in order to get a spaceship to pick him up, Google Suggest needs to talk to Google while you type in order to offer suggestions to you," the company explains on its Web site. "Everything you type, though, is protected by Google’s privacy policy."

Earlier this month, Consumer Watchdog in a letter urged the U.S. Department of Justice to reject Google’s proposed advertising deal with Yahoo. The group cited the lack of user control over Google’s data collection, particularly through Chrome, as the impetus for its opposition to the deal.

Now the organization wants the various State Attorneys General to force Google to let consumers choose to use its services anonymously.

"Google’s role is now unprecedented because the Internet goliath is no longer merely collecting some data about how we search and surf the Web," said Consumer Watchdog president Jamie Court in a statement. "Its new browser and software are actually sending information from inside our computers to its servers. If Google won’t solve its own privacy problems, the company must be prepared for regulators to put the brakes on its unprecedented growth. State Attorneys General need to take action to protect consumers’ privacy and make sure that computer users have the ability to opt-out of Google’s web and browse anonymously." The group wants Google to affix a single prominent button on the main Chrome page that allows the user to enter Incognito mode instantly and to maintain Incognito mode through subsequent sessions until the user chooses to revert to unprotected browsing.

It wants Google users to have a way to extend the Incognito mode to avoid sending information to Google when searching or invoking another action that transmits data.

And it wants Incognito mode to actually hide the user's identity with a default SSL connection, automatic IP anonymization, invisibility to all Google servers including Google Analytics, and the termination of auto-saving, of search suggestions and of external calls to desktop apps and plug-ins related to browsing.

"You should provide the privacy the name implies or stop calling it Incognito mode," the group said in its letter to Google's board.

In response to Consumer Watchdog's complaint, Google said in an e-mailed statement that the organization has misunderstood its products and practices.
Google said it only stores 2% of requests received through Google Suggest, that it anonymizes the IP address of received Suggest data within 24 hours, and that users can turn Suggest off by visiting the Chrome Options menu and clicking the Manage button.

Incognito, according to Google's statement, is intended to prevent information from being left on the user's computer. It is not, in other words, an anonymization service. Google also said that Incognito does not default to SSL (Secure Sockets Layer) "because these connections are provided by Web sites, not browsers, so it is technologically impossible for Google Chrome to behave this way."

The company said that while it disagreed with Consumer Watchdog's video and letter, it remains open to user feedback, particularly with regard to Chrome as it progresses through beta testing.

If you haven't seen Chrome in action yet, take a spin through our Google Chrome image gallery and have a look at the browser that's being touted as a game-changer.
advertising, corporateering, going to court, Google Analytics, Google Chrome, growth, security, Videos, YouTube

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

« Previous Entries

Next Entries »

Search

Search

Recent Posts

Consumer Watchdog, Privacy Rights Clearinghouse File Complaint Over Google's "Deceptive" Privacy Policy Change
Google Renames Robot Car Unit "Waymo" Reminding Us We Need to Know "Way More"
Consumer Watchdog Welcomes FCC's New Broadband Privacy Rules Passed On 3-to-2 Vote
Google Raises 3rd Quarter Lobbying 4.2 Percent to $3.81 Million But Spending Falls Behind AT&T's $4.11 Million; Oracle, Amazon, Microsoft, Facebook Top $2 Million
Robot Car Technology Requires Thorough Testing, Enforceable Safety Standards, Auto Safety Advocates Tell NHTSA Chief

Recent Comments

No comments to show.

Popular
Comments
Tags

- Google's New Scourge Strikes A Nerve
- Extension Lets You Know If Google Is Spying On You
- Google Openness Is A Closed Door -- Open Source Versus An Open Mind
- Dear Google: Harm or Not, You Fouled Up on Privacy
- DOJ's Strict Conditions on Google/ITA Deal Will Open Internet Giant To Unprecedented Scrutiny

Archives

- December 2016
- October 2016
- July 2016
- May 2016
- April 2016
- March 2016
- February 2016
- January 2016
- December 2015

- November 2015
- October 2015
- August 2015
- July 2015
- June 2015
- April 2015
- March 2015
- February 2015
- January 2015
- December 2014
- November 2014
- October 2014
- September 2014
- August 2014
- July 2014
- June 2014
- May 2014
- April 2014
- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013
- July 2013
- April 2013
- March 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011

- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009
- December 2008
- November 2008

Categories

- Action
- Anti-Trust
- Blog Posts
- Clout
- Discussing Search
- Don't Show on Homepage
- In the News
- Petition
- Press Releases
- Privacy
- Videos
- View All

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #252

LAURIE CLARKE SECURITY 20.07.2019 06:00 AM

Google Chrome’s Incognito Mode is way less private than you think

Google Chrome 76 is limiting how you can be tracked in its Incognito Mode. But that doesn't mean you're not being tracked at all

GOOGLE / WIRED

The icon is a detective style hat and glasses, the colour scheme is moody, and many think that entering Google Chrome’s Incognito Mode is like slipping under a cloak of invisibility. Yet it turns out that this is hopelessly misguided. Despite the long-known fact that Incognito isn't truly anonymous, new research has re-emphasised that Google and other web browsers are still tracking you in privacy mode, even on the most sensitive of sites.

A forthcoming research paper, set to be published in the journal New Media & Society and first reported on by the *New York Times*, saw researchers scan 22,484 porn websites. They found 93 per cent of them housed trackers sending information to an average of seven third party domains. While this may be startling many people, incognito has always made for an inadequate privacy tool.

“Private modes in web browsers were never designed as a general privacy fix,” says Lukasz Olejnik, independent cybersecurity and privacy advisor, as well as research associate at the Center for Technology and Global Affairs at Oxford University. “In practice, they offer very little.”

The modes are short-term options that can limit what's recorded on one machine – not an all-encompassing way to be private online. The main functionality of incognito mode is not saving cookies or browser history on the hard disc, meaning that private browsing sessions are isolated from normal ones.
Third party tracking is generally achieved by websites storing cookies on a visitor’s hard drive. Cookies are generally used to track repeat visits from the same user, and build up a profile that’s used to serve ads. In incognito mode, your data is tracked in exactly the same way as normal mode. “The difference is that in ordinary circumstances, trackers are unable to link a "private browsing" session with the "normal session",” says Olejnik. “This means that in principle, after the user closes the browser window no trace should be left.”

But there are of course problems. Notably, third-party sites are able to detect whether site visitors are in private browsing mode, something that Olejnik says is being weaponised against them. It’s this capability that allows, for example, news sites with paywalls to block access to visitors with this mode enabled. If you reach your limit of free articles on the *New York Times*, it's still able to recognise you (and stop access) if you click into incognito.

However, most browsers have never really considered this a major privacy flaw. This is why one loophole that allows third party websites to do this – through Filesystem API detection – has remained in place for so long. The FileSystem API is disabled in Incognito mode, meaning that if a site searches for it and gets an error message, they can determine that a user is in privacy mode. Google has announced the next iteration of its web browser, Chrome 76, will close the loophole. When it's released on July 30, it's probably not going to please publishers.

Read more: How to delete your Google search history and stop tracking

However, despite the loophole being shut, this doesn't mean that Chrome's Incognito Mode will become a better way to browse anonymously. Matthew Forshaw, a lecturer in Data Science at Newcastle University was involved in research that compared the privacy modes of different browsers, and found that a lot of their claims didn't stack up.

This research, conducted back in 2014, uncovered that third party websites were leveraging cookies to identify which users were browsing privately. In normal browsing, cookies are written onto the hard disc itself, whereas in incognito mode, they are held in a device's memory. The research demonstrated that a third party website could remotely instruct someone's browser to write one million cookies, and track how long it took – in a normal browser mode it should take a number of seconds, but when using private mode it’s almost instantaneous.

Another means of determining this mode is almost deceptively simple. Though you may be in private mode, there will only be so many people running the same version of your operating system with that version of the browser. From this information alone, trackers can often identify more personally sensitive and identifiable information. Forshaw says internet users can use a programme called Panoptoclick to obtain a ‘uniqueness score’ – ostensibly telling you how easily identifiable you are as you browse the web. The research project is run by the Electronic Frontier Foundation.

Is your browsing history at least safe from family members or partners who may have access to your computer? Forshaw’s research found that someone with access to your machine could discover which websites had been browsed with easily available tools. On the hard disc and in the memory, there were traces of which websites had been visited when in incognito mode.

But is this all of this by design? From its inception, Google’s whole business model has been predicated on collecting vast collections of data about its users. To create a truly private browsing option where no data is tracked would run directly counter to the tech giant’s raison d’etre. However, Google doesn’t claim that incognito is a catch-all security salve. In fact, it highlights that your activity might still be visible to the websites that you visit, your employer or school (if you are accessing content via an institution’s internet connection) and your internet service provider.

However, when it comes to third party tracking, Forshaw dismantles the notion that these entities may end up capturing such data ‘by accident’. “There's a possibility than one of these trackers makes a decision about what they consider in and out of scope, and that through technical fluke, they end up capturing more information than they intended," he says, "but in general, it's probably very well considered."

Given privacy modes don't guarantee a true layer of anonymity, it's not surprising that they offer no protection higher up the food chain. Your activity will still be available to your internet service provider which can monitor your activity using your public IP address.

There are other options though. If you're looking for a more private online experience, you want to consider a privacy-first web browser. You'll get the most protection by using Tor, which reroutes and encrypts your online activity in multiple layers, but other alternatives such as Brave and DuckDuckGo collect less data than Google's offering.

More great stories from WIRED

🕵️ **It's time you ditched Chrome for a privacy-first web browser**

🚕 **London's minicabs have a cunning plan to beat Uber**

🎉 **A vaccine for Alzheimer's is on the verge of reality**

🤦‍♀️ **Reddit's 'Am I the Asshole' is your new guilty pleasure**

📧 **Get the best tech deals and gadget news in your inbox**

TOPICS PRIVACY SECURITY TECHNOLOGY GOOGLE

MORE FROM WIRED UK

SECURITY

Deepfake Porn Is Out of Control

New research shows the number of deepfake videos is skyrocketing—and the world's biggest search engines are funneling clicks to dozens of sites dedicated to the nonconsensual fakes.

BY MATT BURGESS

BUSINESS

Millions of Workers Are Training AI Models for Pennies

From the Philippines to Colombia, low-paid workers label training data for AI models used by the likes of Amazon, Facebook, Google, and Microsoft.

BY NIAMH ROWE

CULTURE

The 40 Best Films on Netflix This Week

From *The Pale Blue Eye* to *El Conde*, here are our picks for the best streaming titles to feast your eyes on.

BY MATT KAMEN

GEAR

How China's EV Boom Caught Car Companies Napping

Auto execs in the US, Europe, and Japan never thought Chinese EVs were a threat. Now they're coming to wipe the floor with their Western counterparts.

BY CARLTON REID

CULTURE

The 13 Best Films on Amazon Prime Right Now

From *Red, White, and Royal Blue* to *A Million Miles Away*, these are the must-watch films on the streamer.

BY WIRED

CULTURE

The 28 Best Series on Amazon Prime Right Now

From *Jack Ryan* to *Gen V*, these are our picks for what you should be watching on the streamer.

BY MATT KAMEN

CULTURE

The 40 Best Shows on Disney+ Right Now

From *Ahsoka* to *The Wonder Years*, here's everything you should be watching on Disney+.

BY WIRED

CULTURE

The 55 Best Films on Disney+ Right Now

From *The Little Mermaid* to *The Nightmare Before Christmas*, here's what you need to watch on the streaming platform.

BY WIRED

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #326

A Study on Private Browsing: Consumer Usage, Knowledge, and Thoughts

January 2017

Table of Contents

Introduction

At DuckDuckGo, our vision is to raise the standard of trust online. To that end, we strive to understand what people know about online privacy and how they use the privacy features available to them. This report focuses on the feature in web browsers commonly referred to as “Private Browsing.”

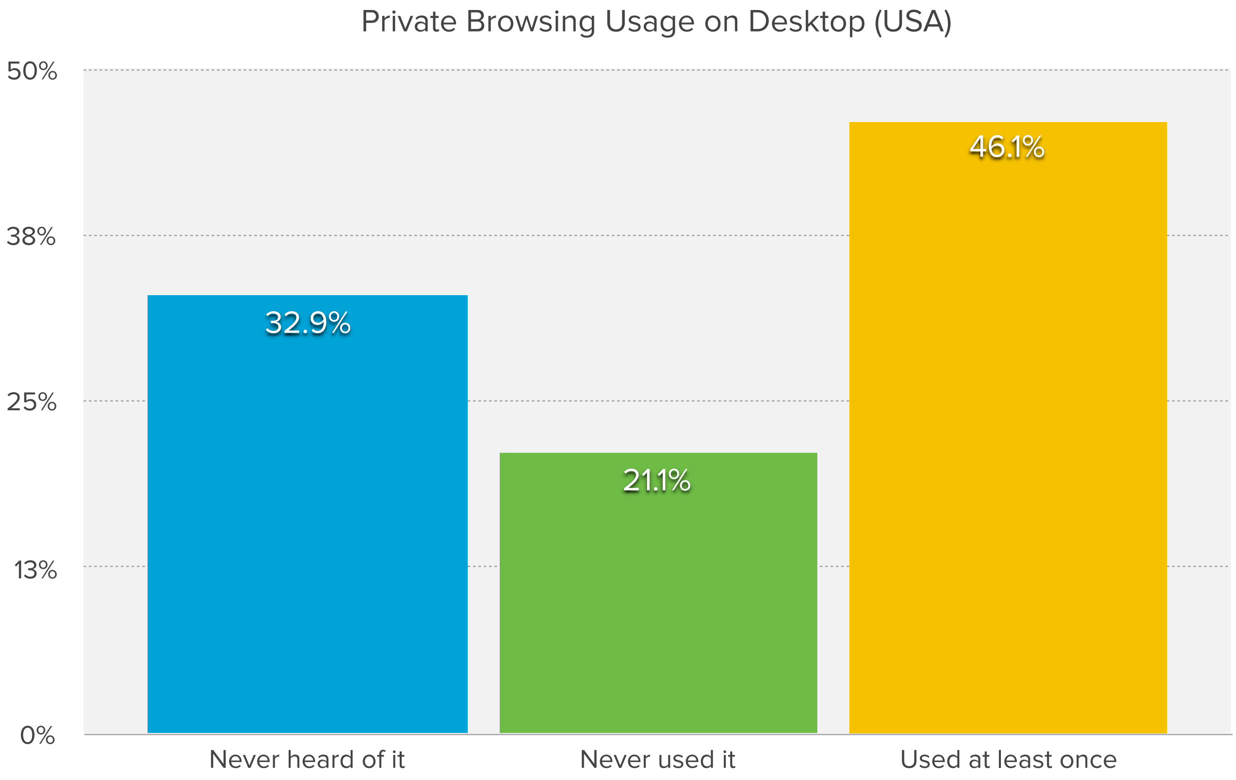
“Private Browsing,” “Privacy Mode,” “Secret Mode,” or “Incognito Mode” is a system of web browsing that clears browsing history and file cache after use. Despite Private Browsing being one of the most commonly known and used privacy features, we find that most people misunderstand the privacy protections it provides.

Our findings are based on a survey conducted with a random sampling of 5,710 Americans who were asked to share their experiences with Private Browsing.

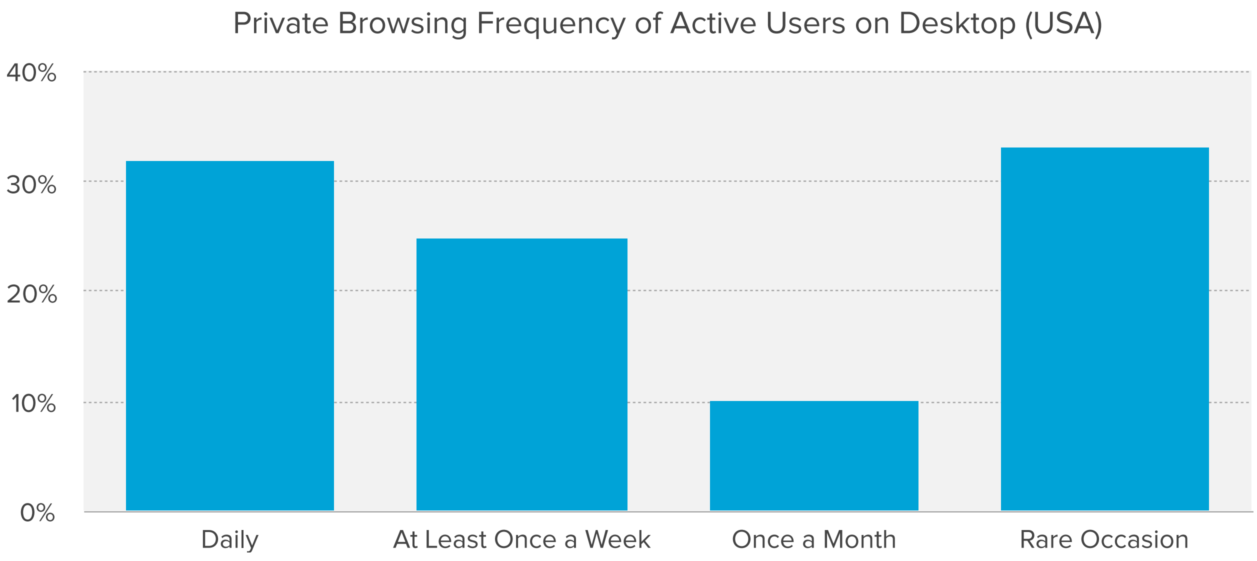
How Do People Use Private Browsing?

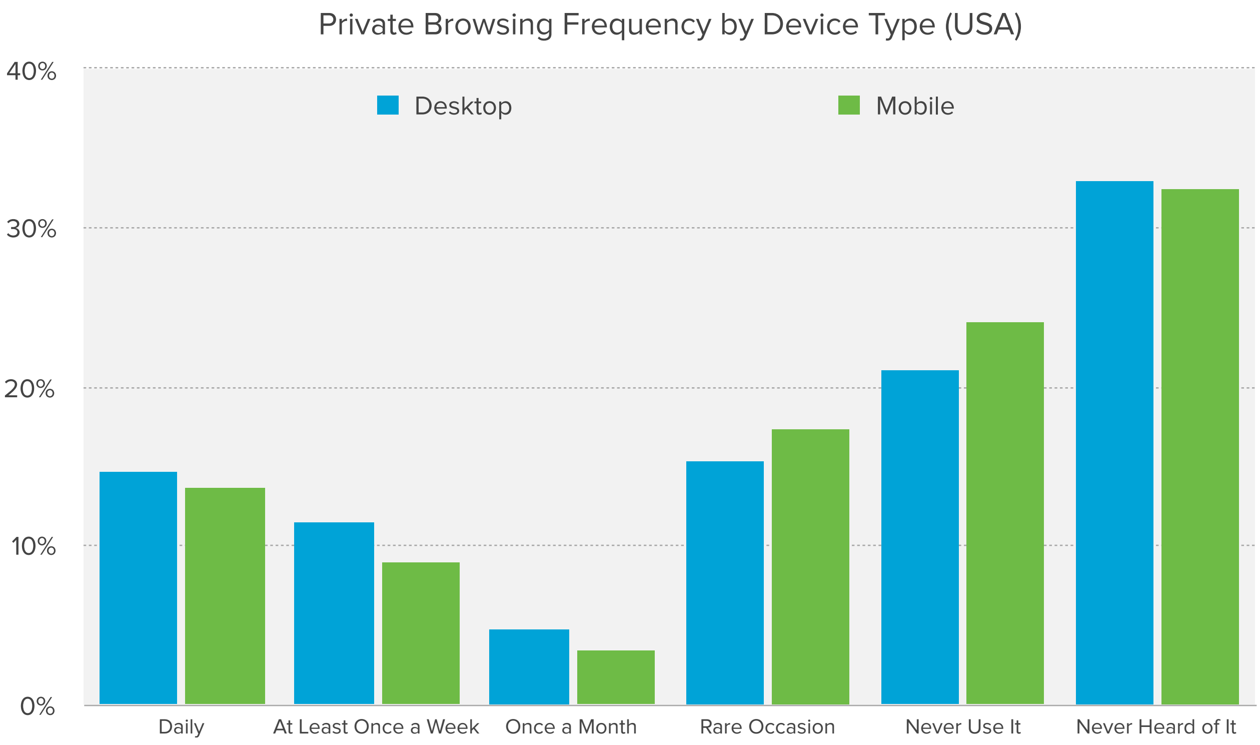
46% of Americans have used Private Browsing.

On desktop, we found that 46.1 ±1.7% of people have used a *"Private Browsing Mode"* at least once, and on mobile that number is 43.5 ±2.7%.

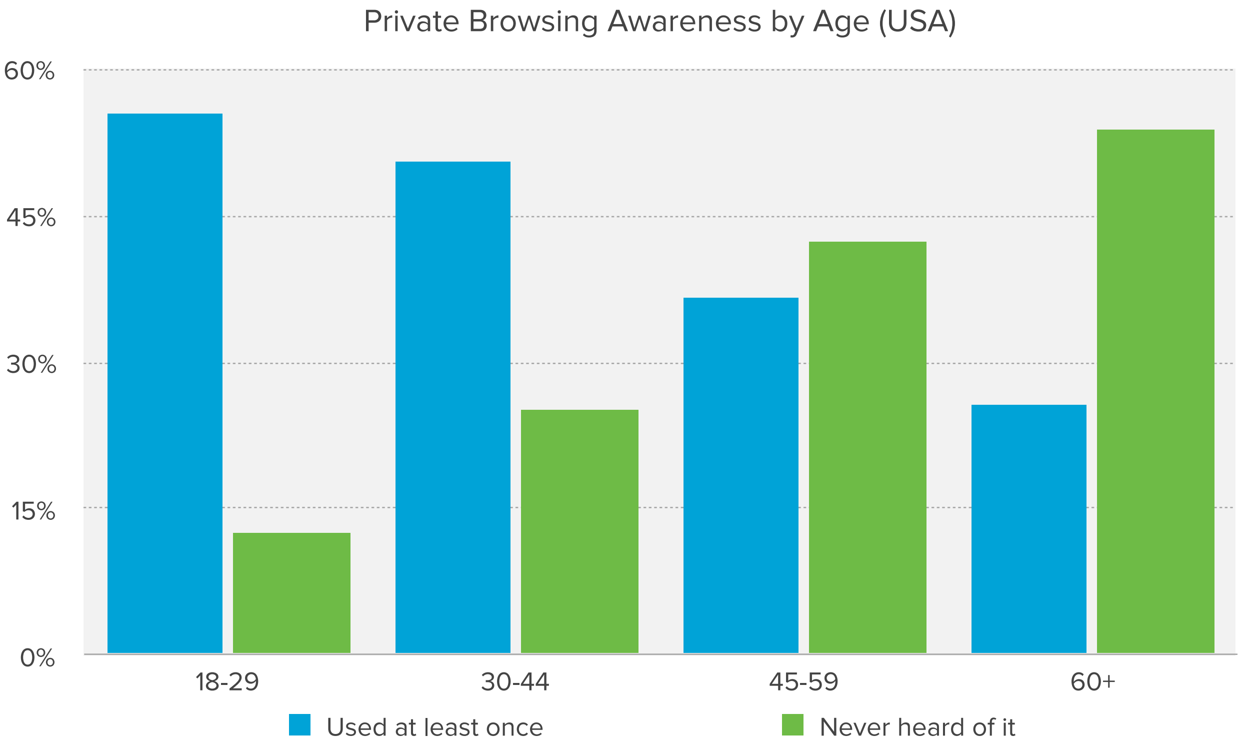


Of those who have used Private Browsing on desktop, 32.9 ±2.3% report using it “*Daily*,” while another 24.8 ± 2.1% report using it “*At Least Once a Week*.” On mobile, 31.5 ±3.9% report “*Daily*” usage, while another 20.6 ±3.3% report usage of “*At Least Once a Week*.”





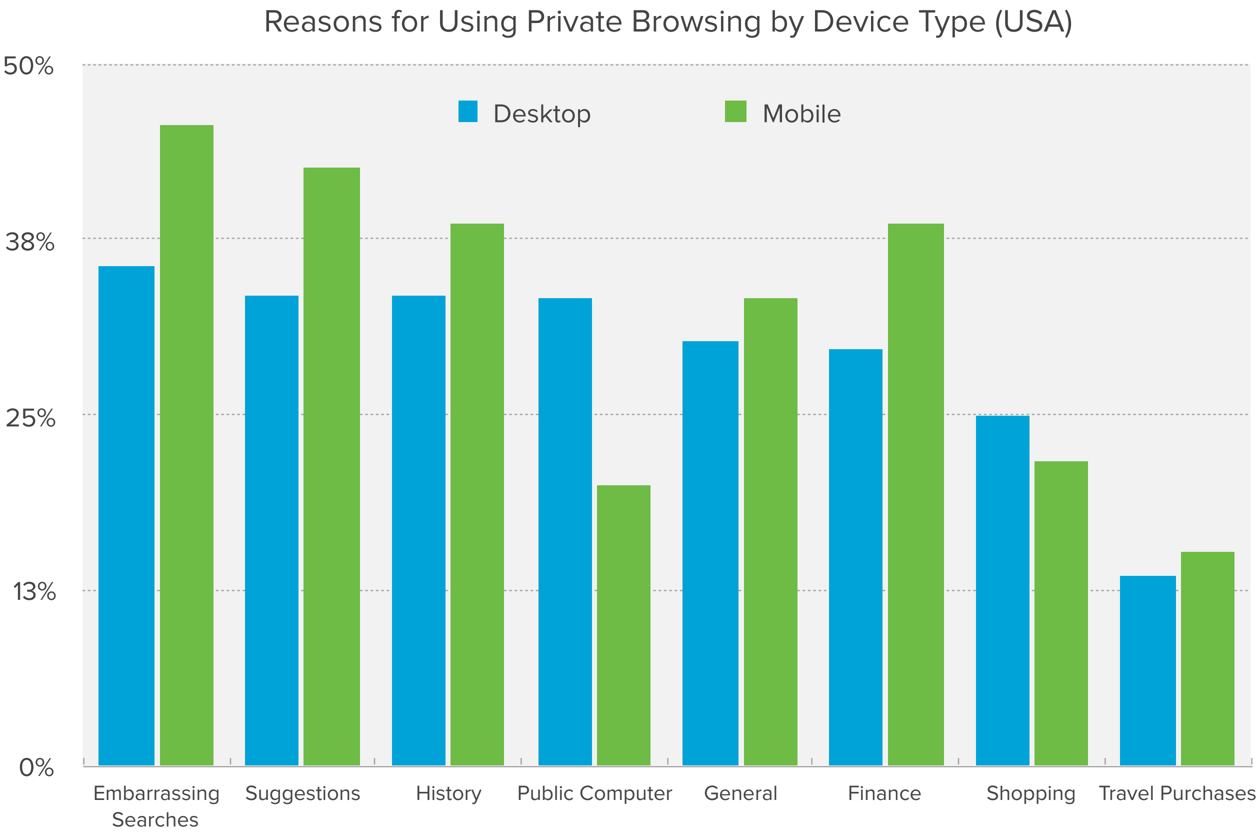
Younger people (18-29) are five times more likely to have heard of Private Browsing than older people (60+), but only twice as likely to have used it. This suggests that older audiences, while less likely to know about Private Browsing, adopt it more frequently once they hear about it.



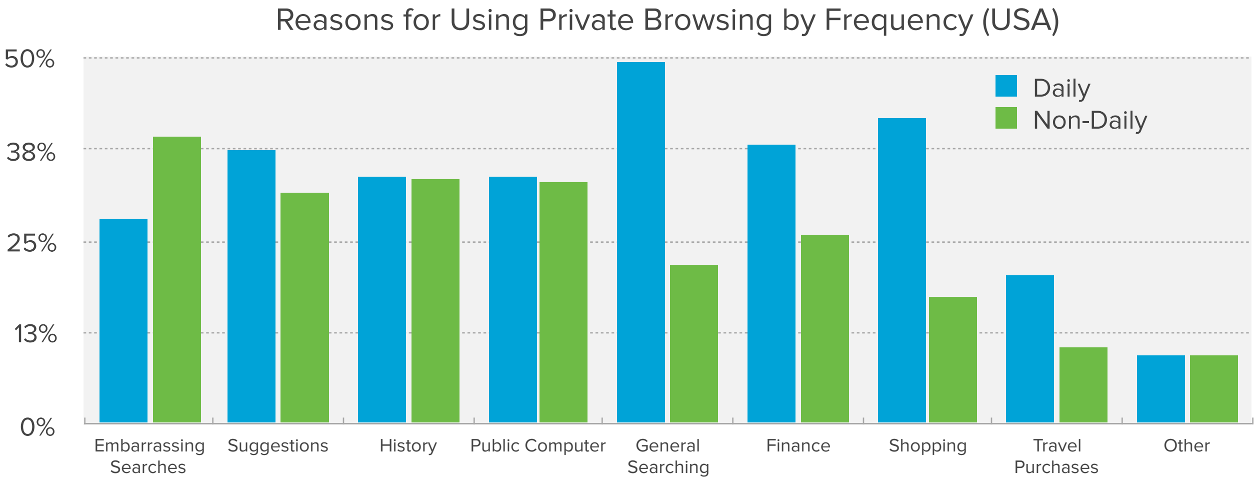
Why Do People Use Private Browsing?

The number one reason people use Private Browsing is "Embarrassing Searches."

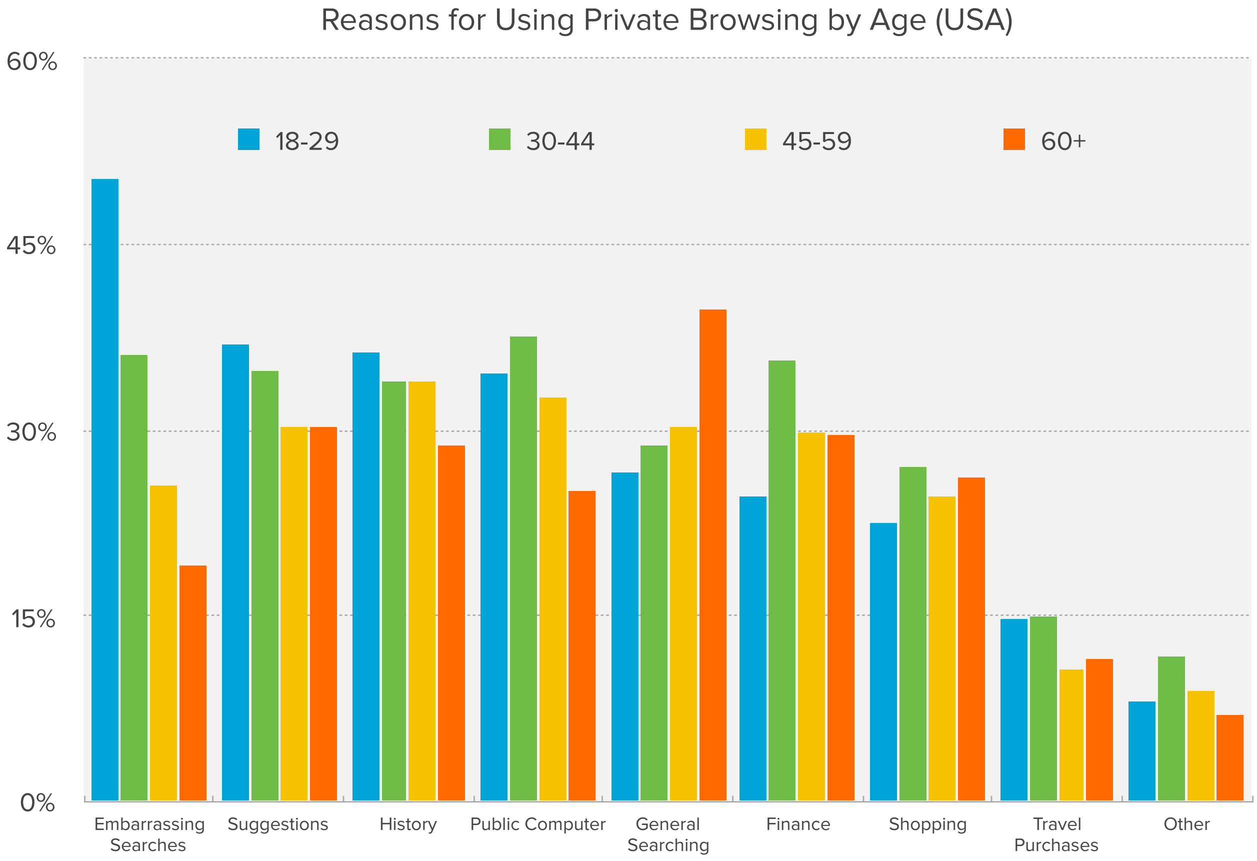
The number one reason people use private browsing is "*Embarrassing Searches*," at 35.7 ±2.5%. Other reasons fell between 24.9 ±2.2% and 33.5 ±2.4%, excluding "*Travel Purchases*," and "*Other*."



People who use Private Browsing daily are two times as likely to use it for “*General Searching*” and about two and half times more likely to use it for “*Shopping*” than non-daily users.



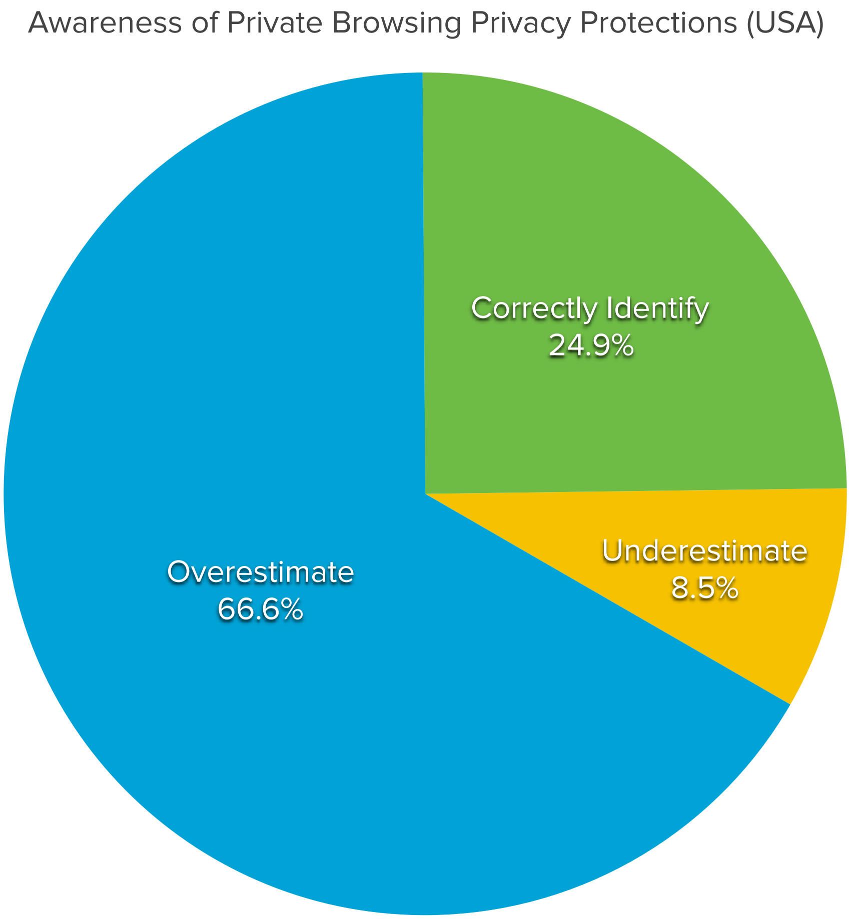
While most reasons for using Private Browsing remain consistent across age brackets, “*Embarrassing Searches*” goes down with age while “*General Searching*” goes up.



What Do People Know About Private Browsing?

76% of Americans who use Private Browsing mode cannot accurately identify the privacy benefit it provides.

75.8 ±2.2% of people who use Private Browsing mode cannot accurately identify the privacy benefit it provides. Of that group, 66.5 ±2.5% overestimate the protection that Private Browsing provides.

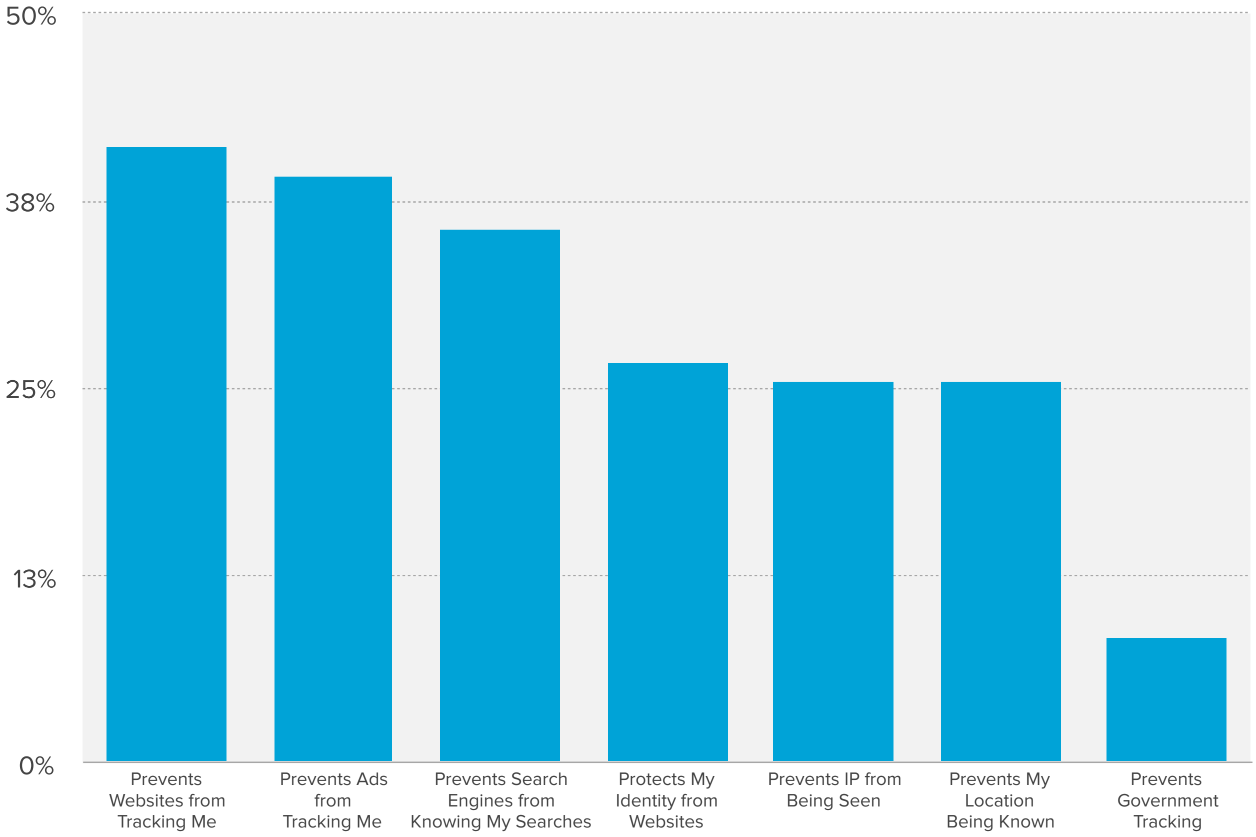


36% of Americans believe that Private Browsing mode prevents a search engine from knowing their searches.

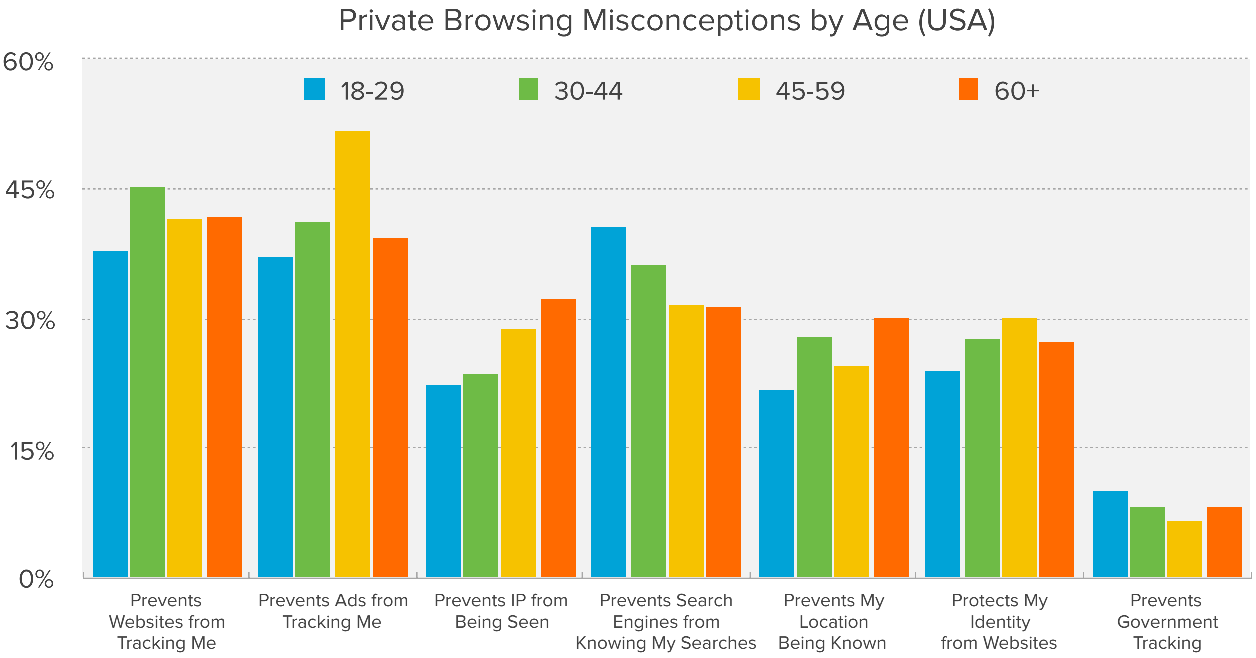
The top 3 misconceptions are:

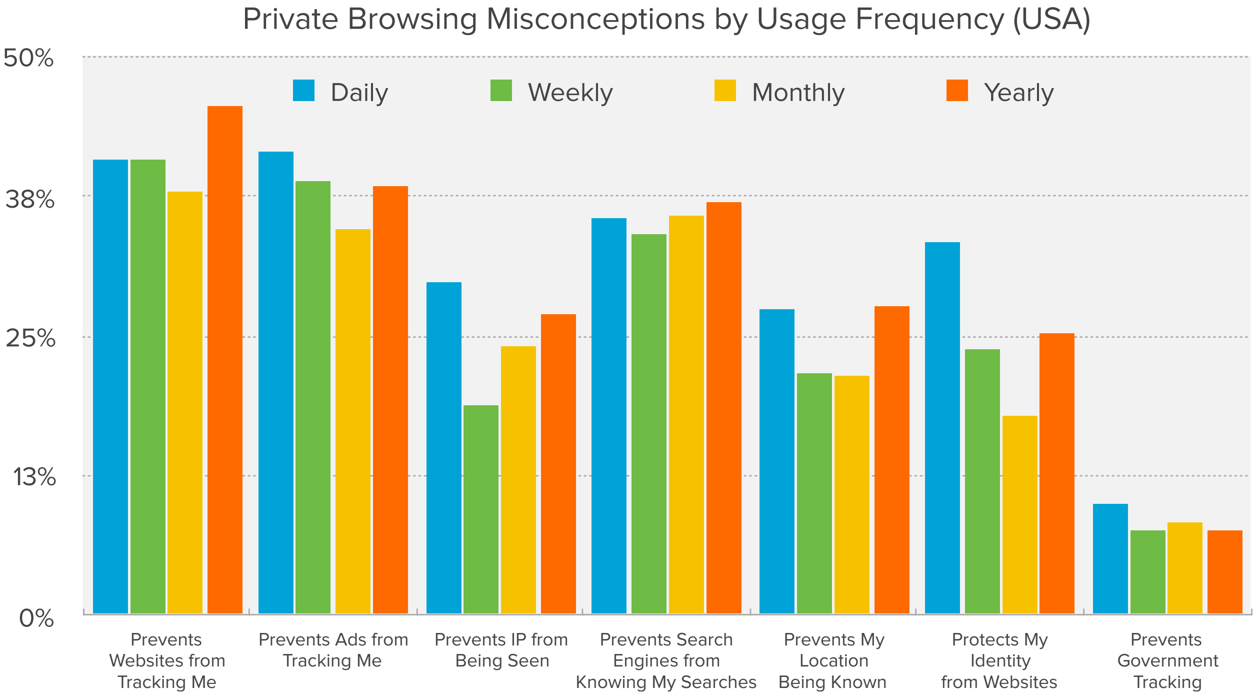
- 41.0 ±2.5% believe that Private Browsing “*Prevents websites from tracking me*.”
- 39.1 ±2.6% believe that Private Browsing “*Prevents ads from tracking me*.”
- 35.7 ±2.5% believe that Private Browsing “*Prevents search engines from knowing my searches*.”

Most Common Misconceptions of Private Browsing (USA)



For the most part, the misconceptions about Private Browsing are consistent. However, younger audiences are more likely to believe a search engine couldn't see their searches in Private Browsing mode, whereas older audiences are more likely to believe that Private Browsing mode would protect their IP address from being seen.





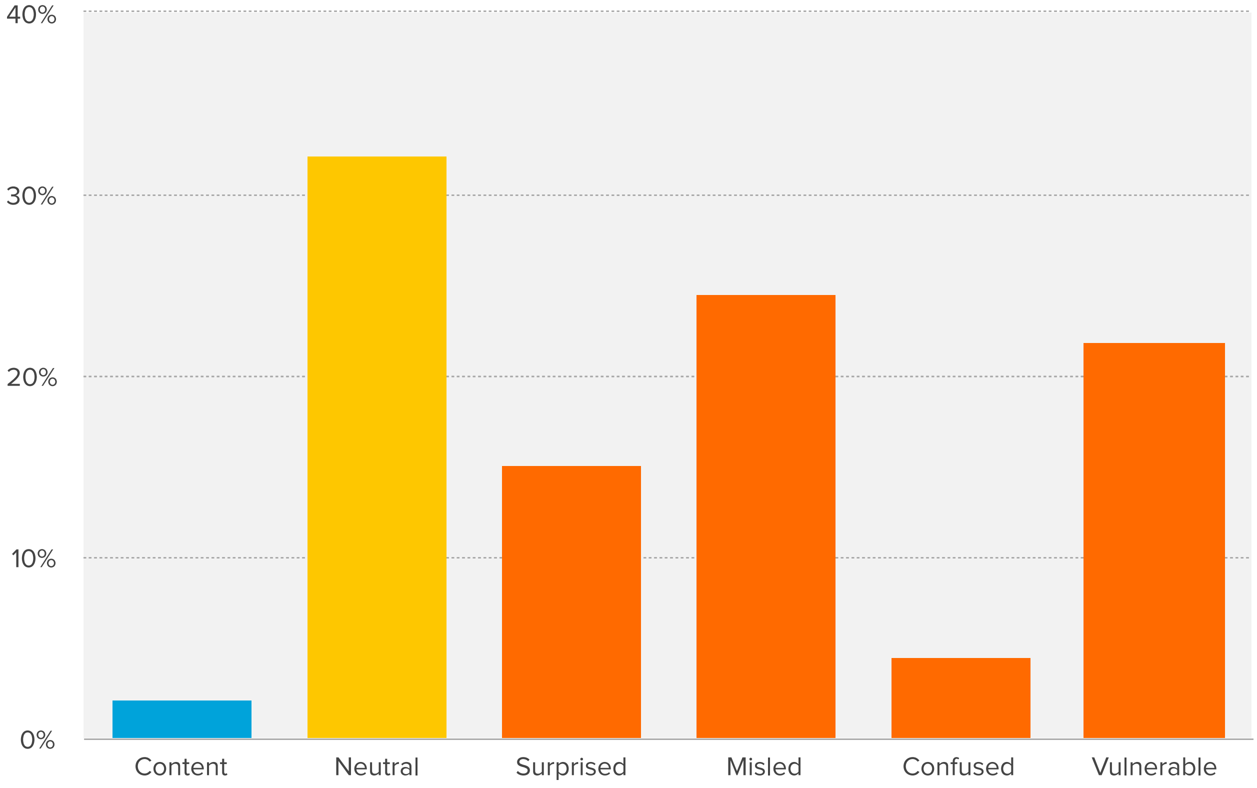
How Do Consumers React to Private Browsing Knowledge?

After asking about Private Browsing usage and knowledge, we informed people about what privacy protections Private Browsing provides, and asked about their emotional reaction:

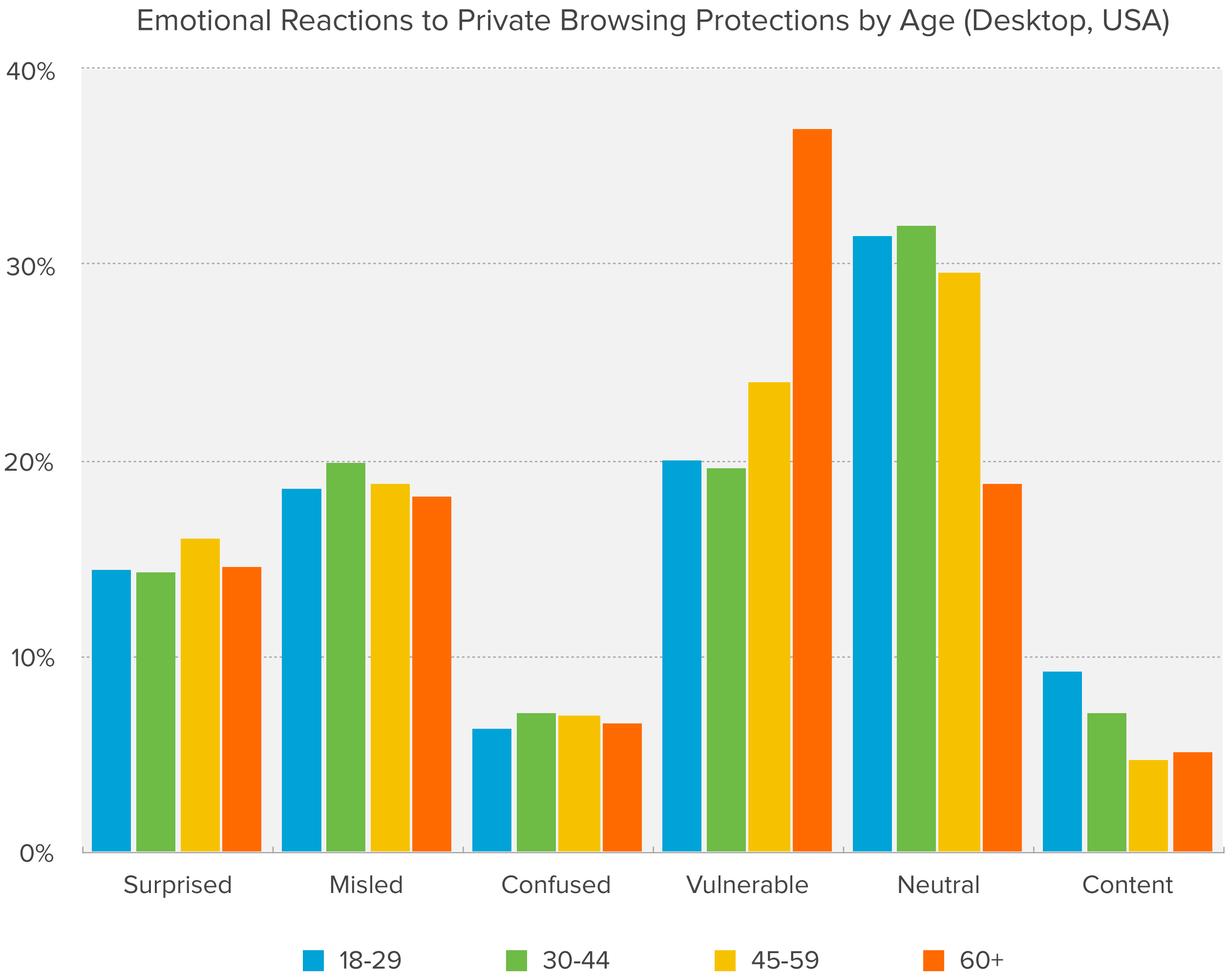
> *Private Browsing mode only prevents your browser history from being recorded on your computer and does not offer any additional protection such as preventing the websites you visit from collecting your information (e.g. your searches on a search engine). How does that make you feel?*

Of the 75.8 ±2.2% of people who have misconceptions about private browsing protections, 65.9 ±2.4% feel “*Surprised*”, “*Misled*”, “*Confused*” or “*Vulnerable*” upon learning about its real protections.

Emotional Reactions to Private Browsing Protections for Desktop (USA)

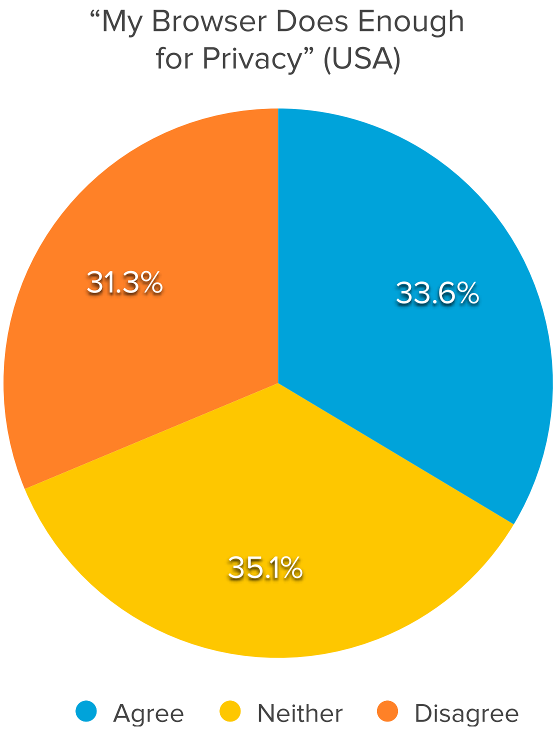


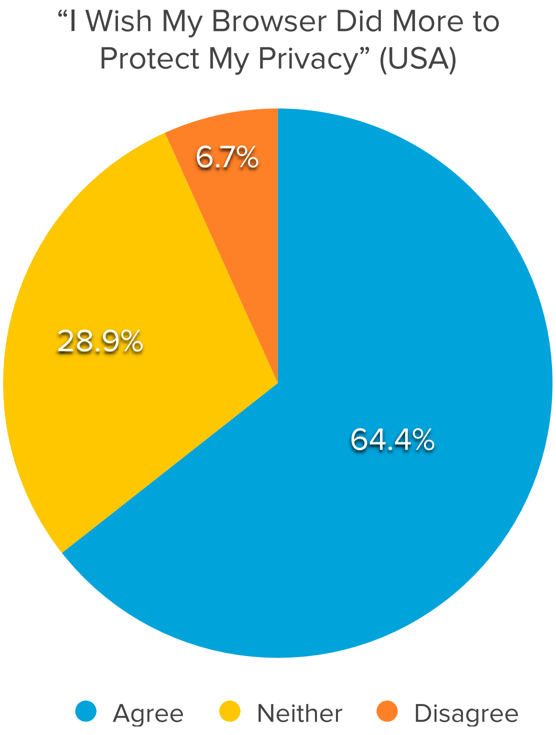
These emotional reactions span age. One notable difference is that 32.1 ±6.4% of people over 60 feel "*Vulnerable*" upon learning about Private Browsing's limitations, vs less than 25% in other age groups.



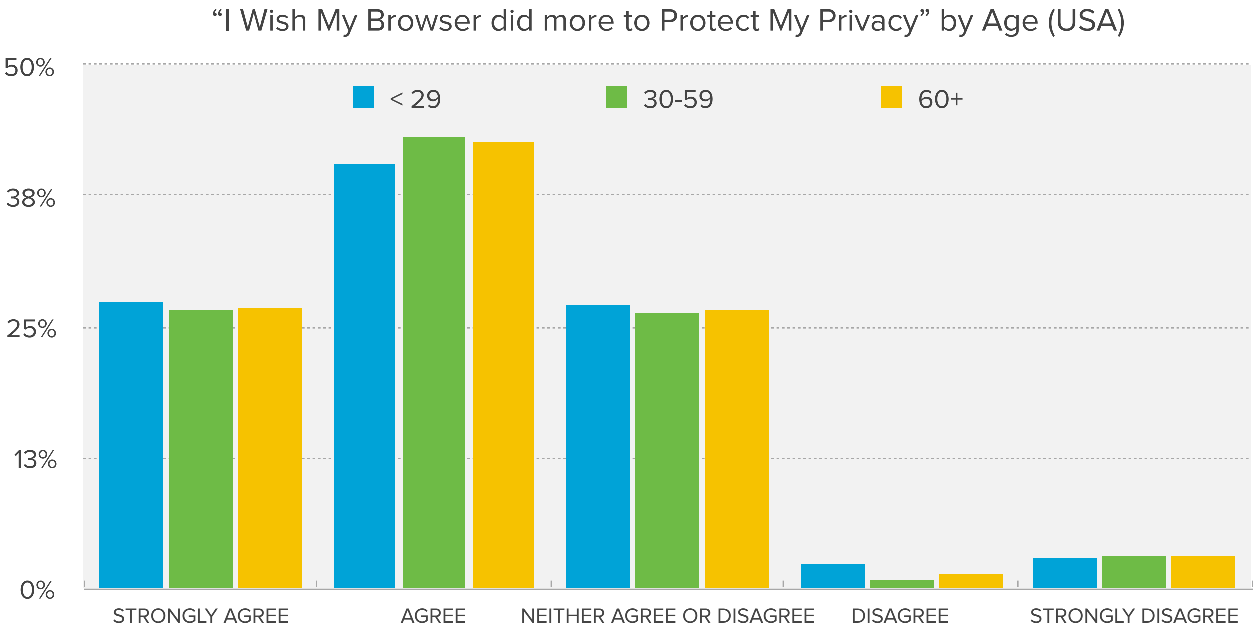
64% of Americans “Agree” or “Strongly Agree” with the statement “I wish my browser did more to protect my privacy.”

When then asked users to agree or disagree with the statement “*My browser does enough to protect my privacy,*” we found a rather even split. When further asked to agree or disagree with the statement “*I wish my browser did more to protect my privacy*,” users were much more strongly in favor of additional privacy protection.

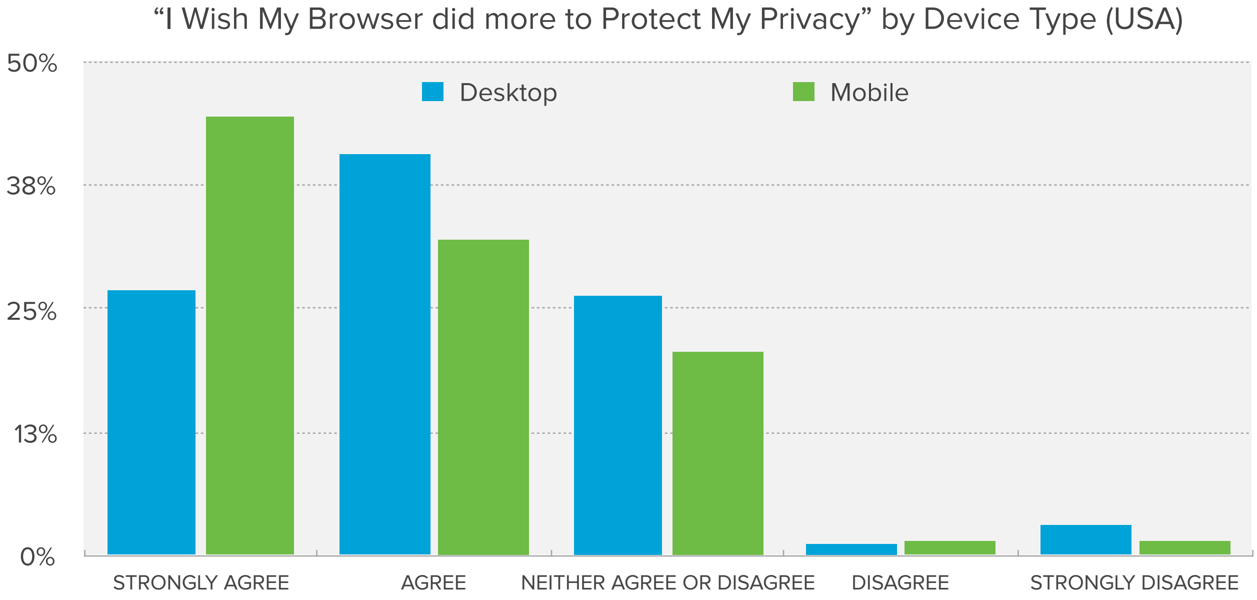




Once again, these findings were consistent across every age group.

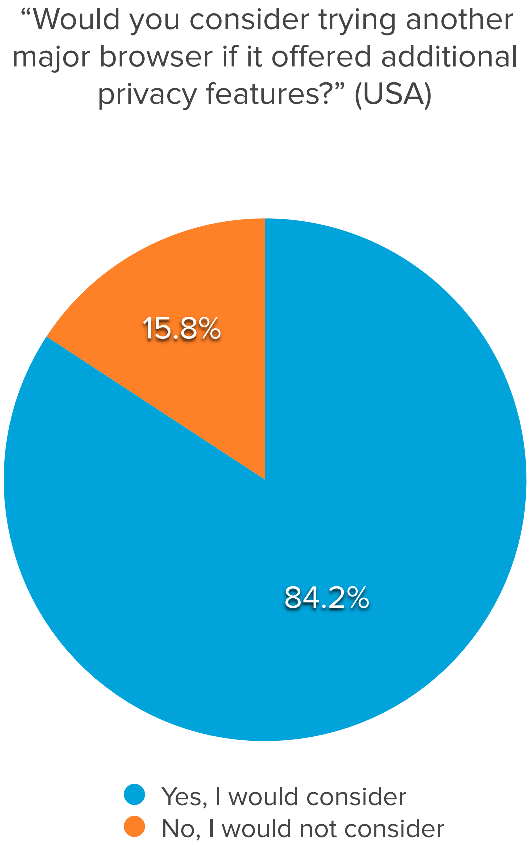


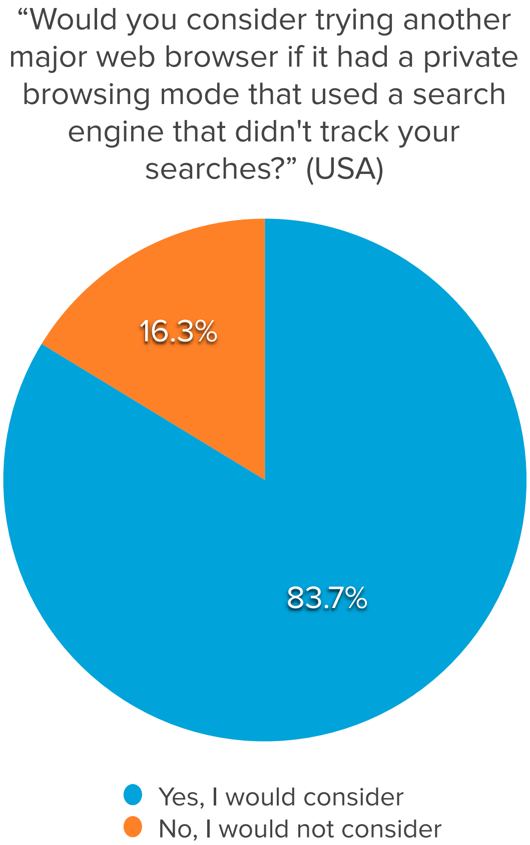
Though when comparing Desktop vs Mobile, we saw a slight skew with mobile users being more likely to "*Strongly Agree*" than *"Agree*."



84% of Americans would consider trying another major web browser if it offered more features to help protect their privacy.

We found people willing to make major changes to better protect their privacy. 84.2 ±1.9% of people say they would "*consider trying another major web browser if it offered more features to help protect your privacy*," and 83.7 ±2.0% say they would "*consider trying another major web browser if it offered a Private Browsing mode that uses a search engine that didn't track your searches*."





Key Takeaways about Private Browsing

1. With 46.1 ± 1.7% of American's having used Private Browsing at least once and 26.7 ±3.0% using it at least once a week, it is clear that Private Browsing is a popular privacy protecting feature.

2. However, 75.8 ±2.2% of people who use Private Browsing incorrectly identify the protection that it provides. As 66.5 ±2.5% overestimate its benefits, this leaves a majority of Private Browsing users exposed more than they think they are.

3. When people find out what private browsing actually does, 65.9 ±2.4% feel "*Surprised*", "*Misled*", "*Confused*" or "*Vulnerable*." 64.0 ±2.6% of people believe their web browser should do more to protect their privacy, and 84.2 ±1.9% are open to trying to a different major web browser if it would provide more privacy protection.

Methodology

These results are based on the polling of a random sample of 5,710 Americans via SurveyMonkey's "Audience" program that "ensures panelists are representative of the U.S. population." Heen, Lieberman and Miethe (2014) confirmed, "Depending on the purpose of the survey research, the average discrepancy rate of 5 to 10% between the particular demographic characteristics of online respondents and their known distribution in the U.S. population may or may not be problematic."[1]

During this survey, respondents reserved the right to decline to answer any survey question. This was allowed in order to prevent biasing answers in the event a user did not understand the question, felt uncomfortable answering the question, or felt there was no answer that accurately represented their response. In these cases of "item non-response," the sample population size was adjusted for that question. A respondent who did not complete all the questions still had their responses included in questions they did complete. The only exception are statements made in this survey that required responses from more than one question.

Respondents were compensated for participation in this survey.

[1] http://www.unlv.edu/sites/default/files/page_files/27/ComparisonDifferentOnlineSampling.pdf

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #367

LAURIE CLARKE SECURITY 20.07.2019 06:00 AM

Google Chrome's Incognito Mode is way less private than you think

Google Chrome 76 is limiting how you can be tracked in its Incognito Mode. But that doesn't mean you're not being tracked at all

GOOGLE / WIRED

The icon is a detective style hat and glasses, the colour scheme is moody, and many think that entering Google Chrome's Incognito Mode is like slipping under a cloak of invisibility. Yet it turns out that this is hopelessly misguided. Despite the long-known fact that Incognito isn't truly anonymous, new research has re-emphasised that Google and other web browsers are still tracking you in privacy mode, even on the most sensitive of sites.

A forthcoming research paper, set to be published in the journal New Media & Society and first reported on by the *New York Times*, saw researchers scan 22,484 porn websites. They found 93 per cent of them housed trackers sending information to an average of seven third party domains. While this may be startling many people, incognito has always made for an inadequate privacy tool.

“Private modes in web browsers were never designed as a general privacy fix,” says Lukasz Olejnik, independent cybersecurity and privacy advisor, as well as research associate at the Center for Technology and Global Affairs at Oxford University. “In practice, they offer very little.”

The modes are short-term options that can limit what's recorded on one machine – not an all-encompassing way to be private online. The main functionality of incognito mode is not saving cookies or browser history on the hard disc, meaning that private browsing sessions are isolated from normal ones.
Third party tracking is generally achieved by websites storing cookies on a visitor’s hard drive. Cookies are generally used to track repeat visits from the same user, and build up a profile that’s used to serve ads. In incognito mode, your data is tracked in exactly the same way as normal mode. “The difference is that in ordinary circumstances, trackers are unable to link a "private browsing" session with the "normal session",” says Olejnik. “This means that in principle, after the user closes the browser window no trace should be left.”

But there are of course problems. Notably, third-party sites are able to detect whether site visitors are in private browsing mode, something that Olejnik says is being weaponised against them. It’s this capability that allows, for example, news sites with paywalls to block access to visitors with this mode enabled. If you reach your limit of free articles on the *New York Times*, it's still able to recognise you (and stop access) if you click into incognito.

However, most browsers have never really considered this a major privacy flaw. This is why one loophole that allows third party websites to do this – through Filesystem API detection – has remained in place for so long. The FileSystem API is disabled in Incognito mode, meaning that if a site searches for it and gets an error message, they can determine that a user is in privacy mode. Google has announced the next iteration of its web browser, Chrome 76, will close the loophole. When it's released on July 30, it's probably not going to please publishers.

Read more: How to delete your Google search history and stop tracking

However, despite the loophole being shut, this doesn't mean that Chrome's Incognito Mode will become a better way to browse anonymously. Matthew Forshaw, a lecturer in Data Science at Newcastle University was involved in research that compared the privacy modes of different browsers, and found that a lot of their claims didn't stack up.

This research, conducted back in 2014, uncovered that third party websites were leveraging cookies to identify which users were browsing privately. In normal browsing, cookies are written onto the hard disc itself, whereas in incognito mode, they are held in a device's memory. The research demonstrated that a third party website could remotely instruct someone's browser to write one million cookies, and track how long it took – in a normal browser mode it should take a number of seconds, but when using private mode it’s almost instantaneous.

Another means of determining this mode is almost deceptively simple. Though you may be in private mode, there will only be so many people running the same version of your operating system with that version of the browser. From this information alone, trackers can often identify more personally sensitive and identifiable information. Forshaw says internet users can use a programme called Panoptoclick to obtain a ‘uniqueness score’ – ostensibly telling you how easily identifiable you are as you browse the web. The research project is run by the Electronic Frontier Foundation.

Is your browsing history at least safe from family members or partners who may have access to your computer? Forshaw’s research found that someone with access to your machine could discover which websites had been browsed with easily available tools. On the hard disc and in the memory, there were traces of which websites had been visited when in incognito mode.

But is this all of this by design? From its inception, Google’s whole business model has been predicated on collecting vast collections of data about its users. To create a truly private browsing option where no data is tracked would run directly counter to the tech giant’s raison d’etre. However, Google doesn’t claim that incognito is a catch-all security salve. In fact, it highlights that your activity might still be visible to the websites that you visit, your employer or school (if you are accessing content via an institution’s internet connection) and your internet service provider.

However, when it comes to third party tracking, Forshaw dismantles the notion that these entities may end up capturing such data ‘by accident’. “There's a possibility than one of these trackers makes a decision about what they consider in and out of scope, and that through technical fluke, they end up capturing more information than they intended," he says, "but in general, it's probably very well considered."

Given privacy modes don't guarantee a true layer of anonymity, it's not surprising that they offer no protection higher up the food chain. Your activity will still be available to your internet service provider which can monitor your activity using your public IP address.

There are other options though. If you're looking for a more private online experience, you want to consider a privacy-first web browser. You'll get the most protection by using Tor, which reroutes and encrypts your online activity in multiple layers, but other alternatives such as Brave and DuckDuckGo collect less data than Google's offering.

More great stories from WIRED

🕵️ **It's time you ditched Chrome for a privacy-first web browser**

🚕 **London's minicabs have a cunning plan to beat Uber**

🎉 **A vaccine for Alzheimer's is on the verge of reality**

🤦 **Reddit's 'Am I the Asshole' is your new guilty pleasure**

📧 **Get the best tech deals and gadget news in your inbox**

TOPICS PRIVACY SECURITY TECHNOLOGY GOOGLE

MORE FROM WIRED UK

SECURITY

Deepfake Porn Is Out of Control

New research shows the number of deepfake videos is skyrocketing—and the world's biggest search engines are funneling clicks to dozens of sites dedicated to the nonconsensual fakes.

BY MATT BURGESS

BUSINESS

Millions of Workers Are Training AI Models for Pennies

From the Philippines to Colombia, low-paid workers label training data for AI models used by the likes of Amazon, Facebook, Google, and Microsoft.

BY NIAMH ROWE

CULTURE

The 40 Best Films on Netflix This Week

From *The Pale Blue Eye* to *El Conde*, here are our picks for the best streaming titles to feast your eyes on.

BY MATT KAMEN

GEAR

How China's EV Boom Caught Car Companies Napping

Auto execs in the US, Europe, and Japan never thought Chinese EVs were a threat. Now they're coming to wipe the floor with their Western counterparts.

BY CARLTON REID

CULTURE

The 13 Best Films on Amazon Prime Right Now

From *Red, White, and Royal Blue* to *A Million Miles Away*, these are the must-watch films on the streamer.

BY WIRED

CULTURE

The 28 Best Series on Amazon Prime Right Now

From *Jack Ryan* to *Gen V*, these are our picks for what you should be watching on the streamer.

BY MATT KAMEN

CULTURE

The 40 Best Shows on Disney+ Right Now

From *Ahsoka* to *The Wonder Years*, here's everything you should be watching on Disney+.

BY WIRED

CULTURE

The 55 Best Films on Disney+ Right Now

From *The Little Mermaid* to *The Nightmare Before Christmas*, here's what you need to watch on the streaming platform.

BY WIRED

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #380

BLOG (/BLOG/) ▸ PRIVACY (/TAG/PRIVACY/)

Understanding how people use private browsing

(https://www.facebook.com/sharer/sharer.php?u=https%3A//elie.net/blog/privacy/understanding-how-peo

(https://twitter.com/intent/tweet/?text=Understanding%20how%20people%20use%20private%20browsir

(https://linkedin.com/sharing/share-offsite/?url=https%3A//elie.net/blog/privacy/understanding-how-peopl

(https://wa.me/?text=https%3A//elie.net/blog/privacy/understanding-how-people-use-private-browsing)

(http://www.reddit.com/submit?url=https%3A//elie.net/blog/privacy/understanding-how-people-use-privat

(mailt
bject=From%20elie.net%3A%20Understanding%20how%20people%20use%20private%20browsing&body=H
w-people-use-private-browsing)

(https://feeds.feedburner.com/inftoint)

SUBSCRIBE

Authors Elie Bursztein Date July 2017 Reading time 5 min

This post looks at how and why people are using the private browsing mode.

Private Browsing (https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history), also known as InPrivate (https://support.microsoft.com/en-us/microsoft-edge/browse-inprivate-in-microsoft-edge-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2) in Internet Explorer and Incognito mode (https://support.google.com/chrome/answer/95464) in Google Chrome, is a special mode where the browser doesn't record the browsing activity on the local device. The promise made to the user is that when the private windows are closed, no trace will be left on the computer. Technically, this is achieved by storing everything related to browsing, including the cache and history, in the RAM and wiping it out when the private browsing windows is closed.

However, having a feature that works as intended does not necessarily mean that users actually know about it, understand what it does, or use it correctly. Making sure that users understand what they are getting out of private browsing has become increasingly important, as a few browsers, such as Firefox (https://www.mozilla.org/en-US/), Brave (https://brave.com/), and Opera (http://www.opera.com/), have decided to add features to private browsing to mitigate web tracking. These additional features, for better or worse, blur the limitations of private browsing and potentially shift users' expectations.

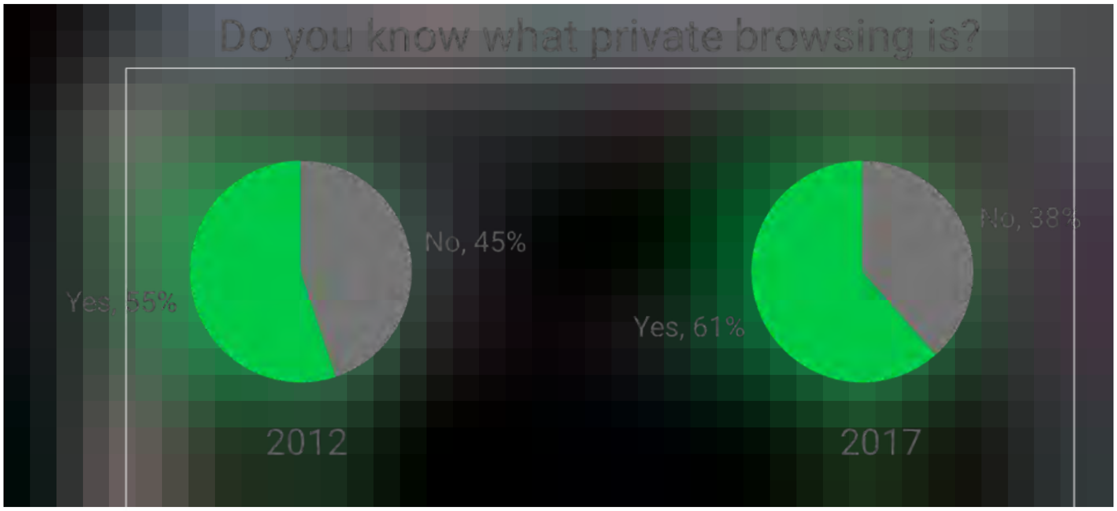
Since our initial research paper (https://elie.net/publication/an-analysis-of-private-browsing-modes-in-modern-browsers) on private browsing and original survey were produced, the landscape has drastically changed, so it was time to run an improved online survey to better understand why users use private browsing and their expectations. Expanding on the original survey, I asked the following questions:

> 1. Do you know what private browsing is, and do you use it?
> 2. What do you use private browsing for?
> 3. Where do you use private browsing?
> 4. Who are you hiding from when you use it?

This post analyzes the results of this survey and, whenever possible, contrasts the responses received in June 2017 with the ones from April 2012 and the DuckDuckGo study (https://spreadprivacy.com/private-browsing-9276d6d16ea4) to understand whether private browsing habits have changed in recent years.

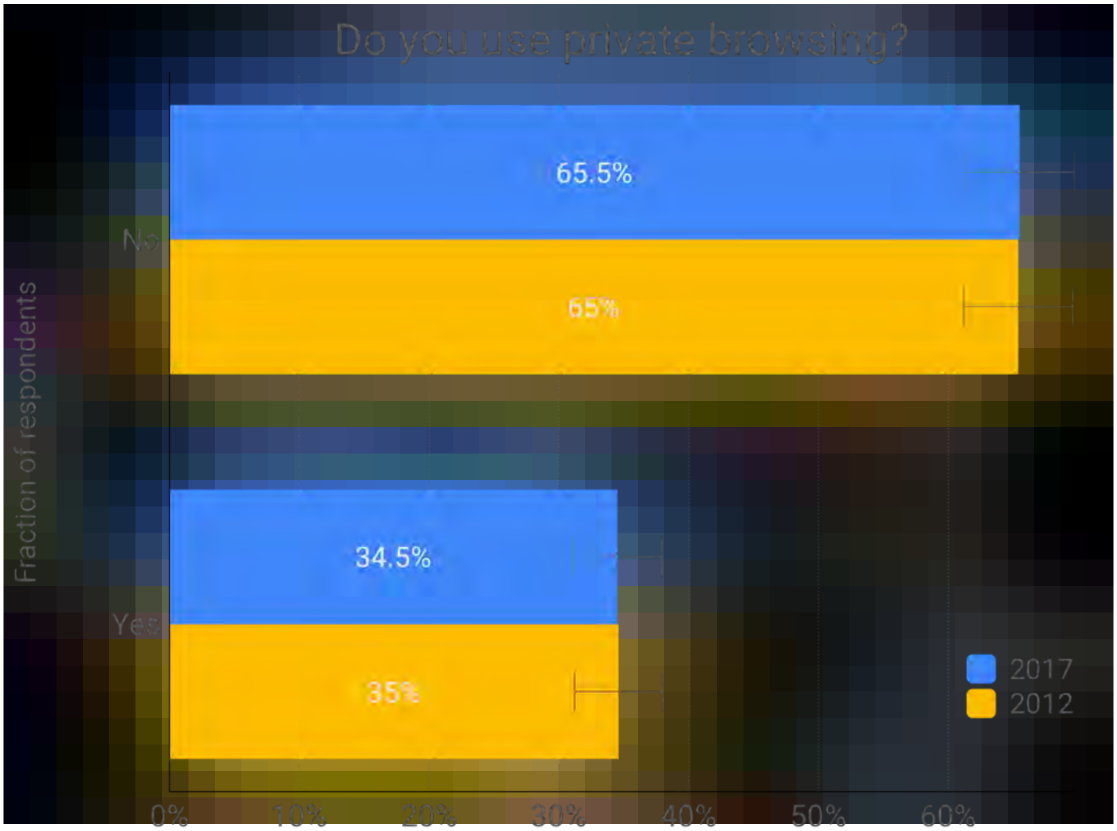
This post also reflects on how the new private browsing features introduced by Opera, Brave, and Firefox potentially help or harm users. The survey was run via Google consumer surveys with at least 200 US respondents for each question.

How many people know about private browsing?



As of 2017, almost two out of three Internet users (61%) think they know what private browsing is, as reported in the pie chart above. This is a 10% increase compared to 2012, which is great because it means that more people know they can use it if they need to. The 2017 survey results are in the ballpark of the DuckDuckGo results (when accounting for variance), which show that 67% of the people surveyed know about private browsing.

How many people use private browsing?

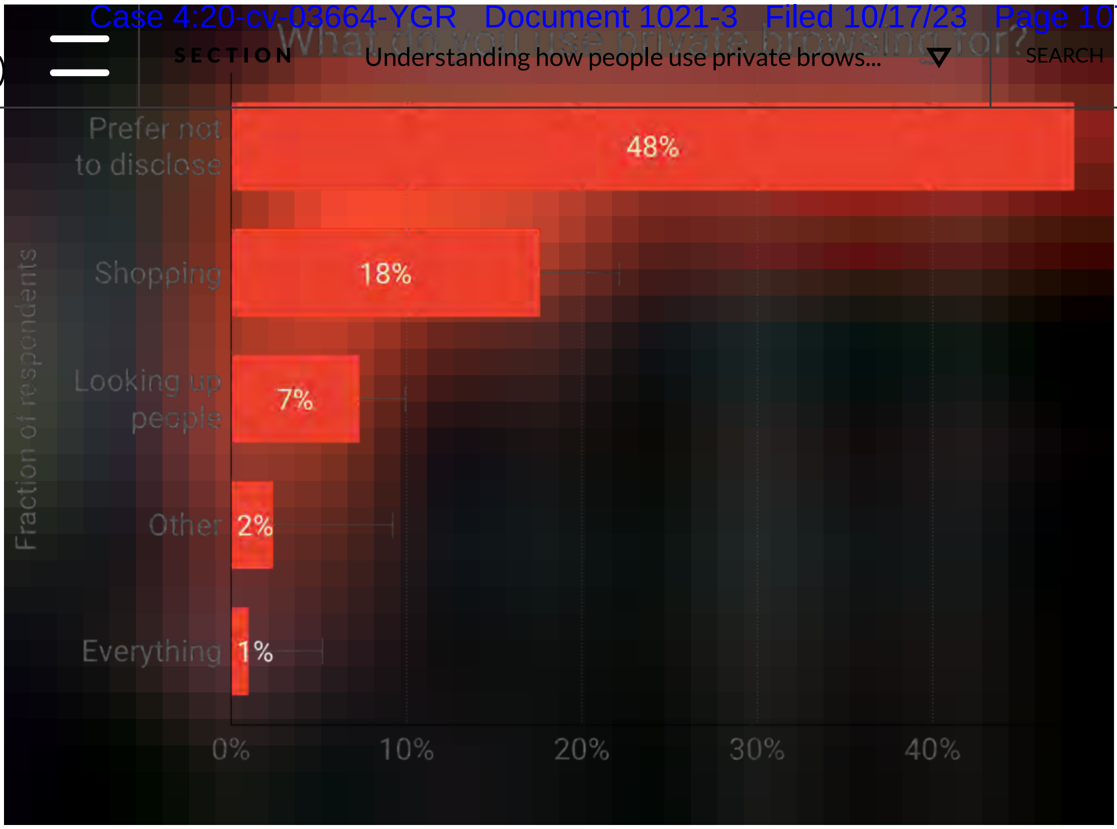


Overall, 20.1% of surveyed users use private browsing, which means that a little over one in three (35%) people who know about private browsing mode use it. I was expecting this number to have increased since 2012 given how much privacy is in the press, but the fraction of people using private browsing has remained almost unchanged.

So how many more people are using private browsing today? Given that the number of people knowing about private browsing has increased by 6% and that one person in three who know about this feature uses it, we can estimate that the number of users has increased by roughly 2%.

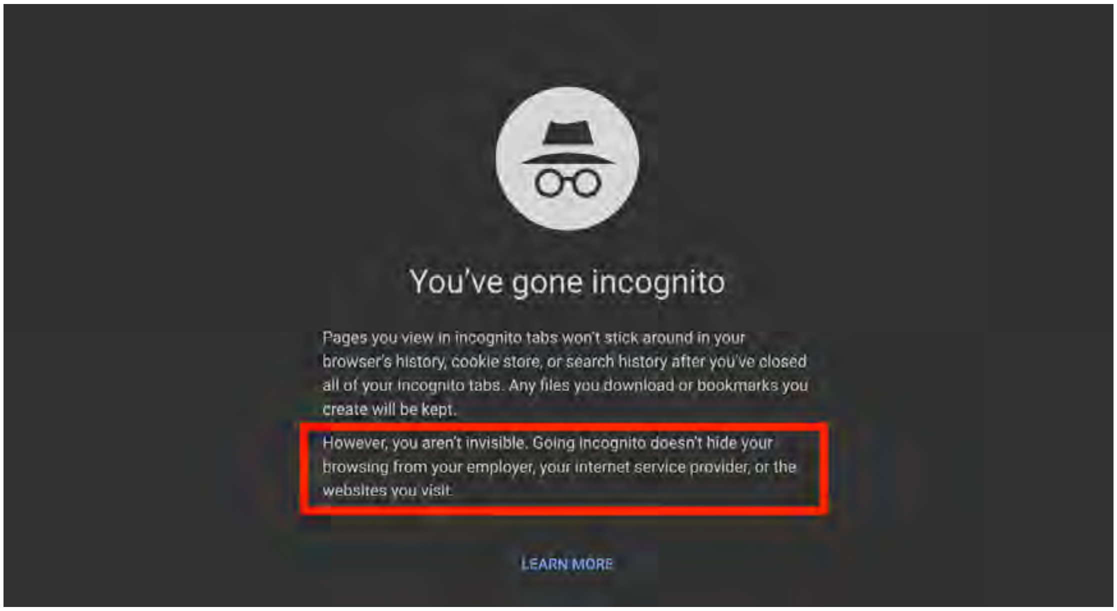
DuckDuckGo asked if people used private browsing “at least once,” so their results are not directly comparable to the survey results. That being said, the results appear to roughly match when considering only people who report using private browsing frequently. For reference, DDG found that roughly 35% of the people used it infrequently.

What do people use private browsing for?



Unsurprisingly, most people refused to answer this question (48%). They mostly use it to search for specific things that they most likely don't want to have in their history and be part of personalized search (37.2%). Surveys are clearly not the best approach to understand why people are using the private browsing mode because of the embarrassment factor.

Who are users hiding from when using private browsing?

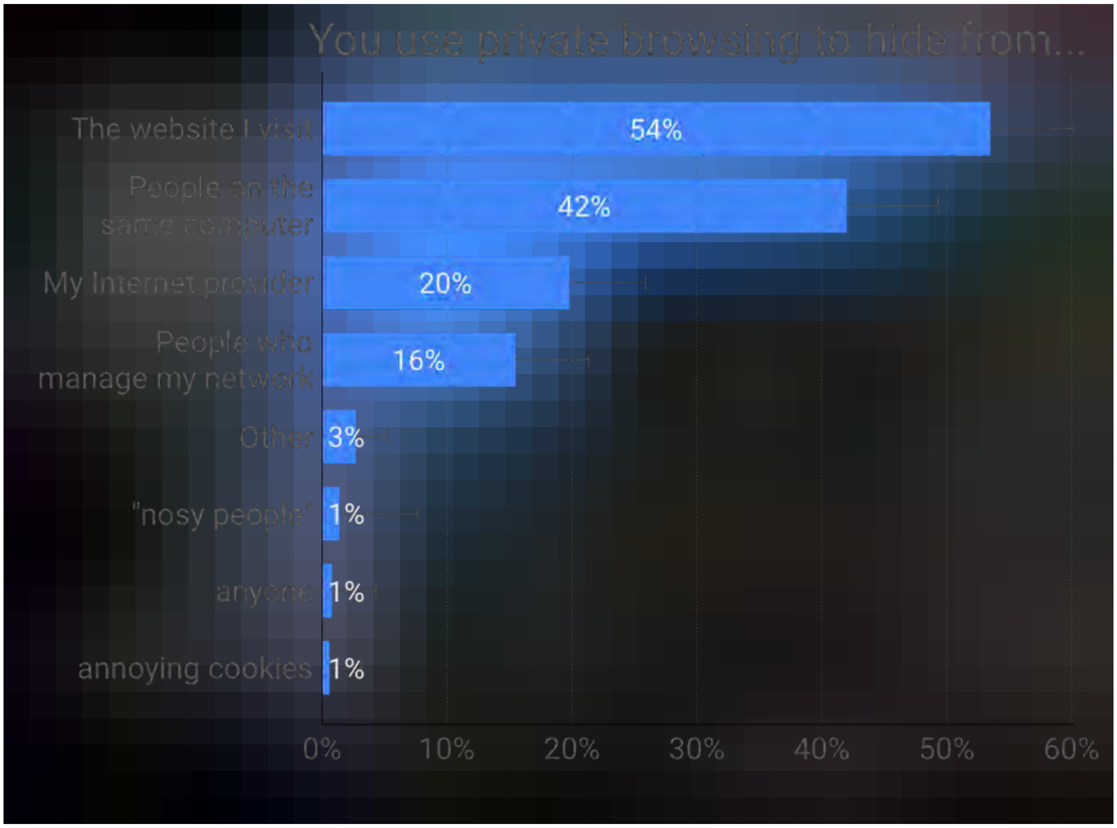


You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

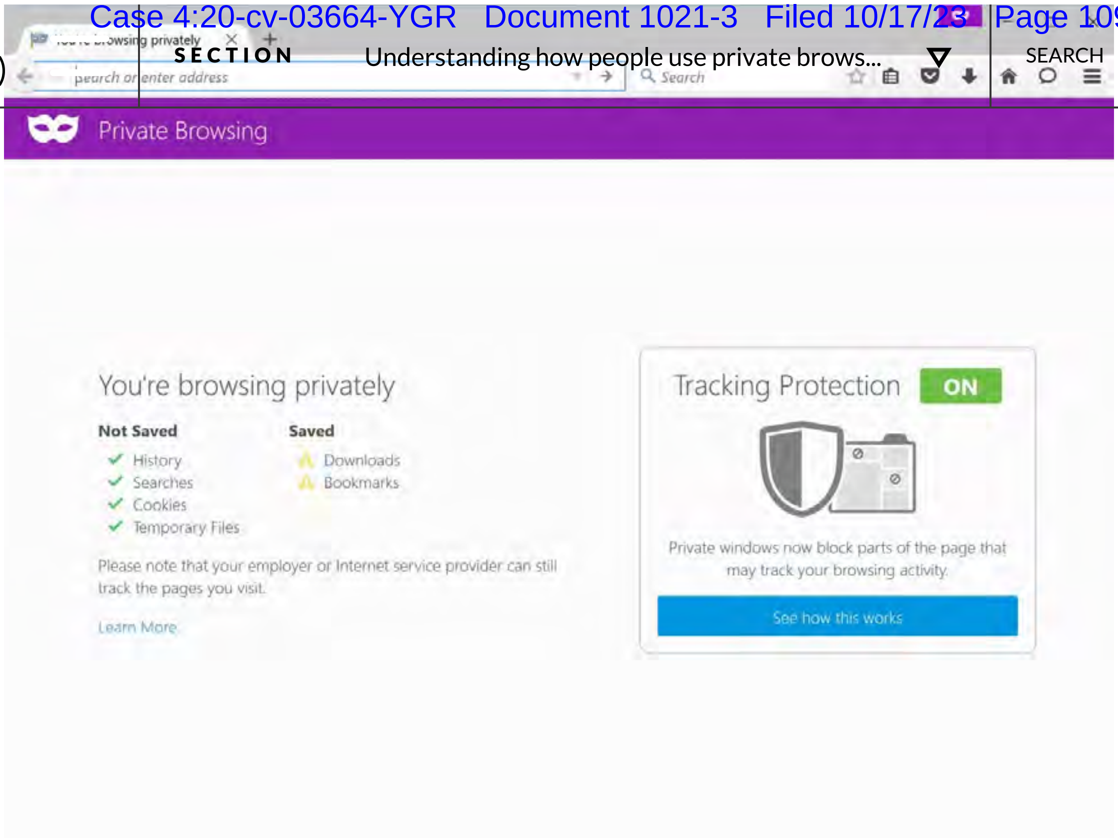
As discussed at length in our research paper about private browsing (https://elie.net/publication/an-analysis-of-private-browsing-modes-in-modern-browsers), a key concern about private browsing is that people might misunderstand what it can protect them from. Browsers try to mitigate this issue by showing a short intro text when people enter a private browsing mode. For example, the screenshot above from Chrome's Incognito mode reminds the user that the incognito mode doesn't prevent ISPs or websites from tracking user's browsing.



Though browsers do their best to inform users of the limitations of private browsing, most of the survey respondents use private browsing for the wrong reasons. Most (53%) use it to protect themselves from the websites they visit, which is not something private browsing is meant for. Only 42% of the respondents claim to use it for its intended purpose, which is not leaving a trace on the local computer. These results emphasize the need to raise awareness of what private browsing can and cannot do (<self-promo>Sharing this post being obviously a great way to help with this :)</self-promo>)

Expanding private browsing functionality

Preventing web tracking is a notoriously difficult if not an impossible task, which is why browsers generally do not try to address it initially to avoid giving the user a false sense of security.



You're browsing privately

Not Saved
- ✓ History
- ✓ Searches
- ✓ Cookies
- ✓ Temporary Files

Saved
- ⚠ Downloads
- ⚠ Bookmarks

Please note that your employer or Internet service provider can still track the pages you visit.

Learn More

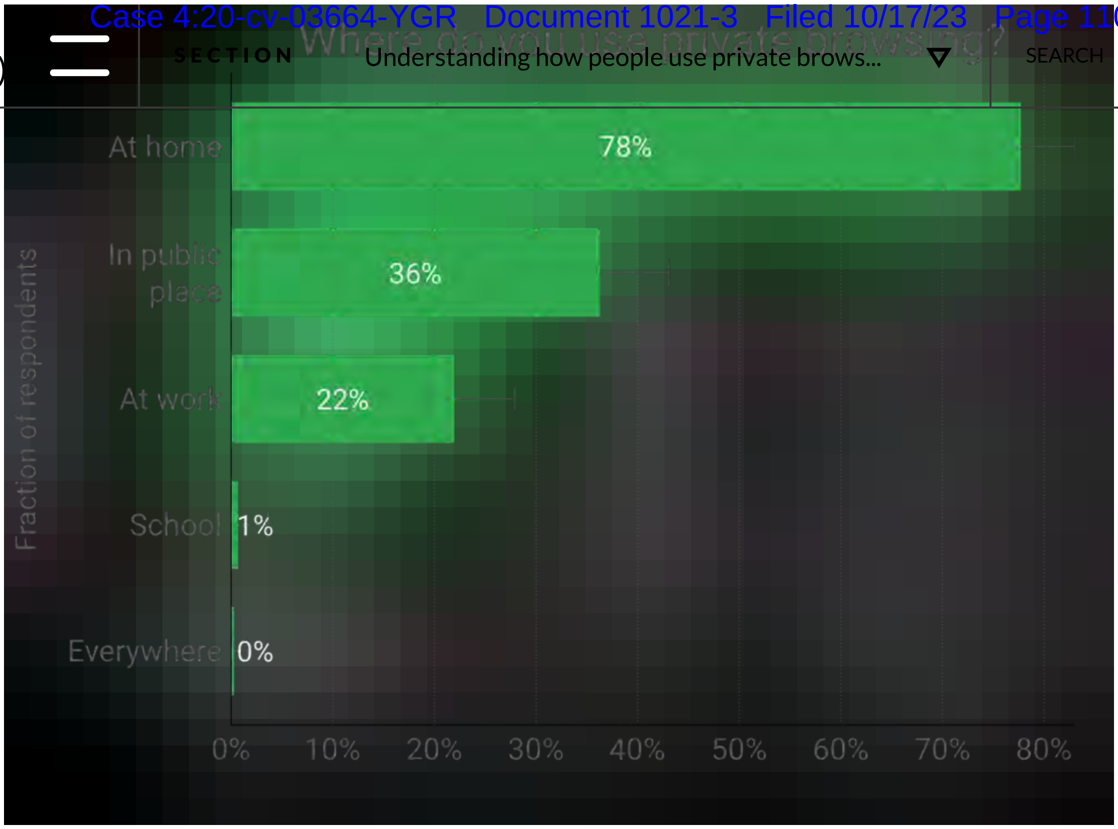
Tracking Protection ON

Private windows now block parts of the page that may track your browsing activity.

However, Firefox, Brave, and Opera have recently decided to try to meet users' expectations by adding features that help reduce website tracking. Firefox, as shown in the screenshot above, disables third-party cookies while using private browsing, whereas Opera offers a free VPN to mask the IP address, and Brave attempts to prevent fingerprinting.

While these features indeed reduce website's' ability to track users, they are far from being foolproof, which leaves us with private browsing modes that only partially do what users want. I am not sure whether this is better than not doing it at all, but it certainly offers users a choice, which is always good. We in the security community should be careful to clarify the limitations of each approach so users can make informed decisions.

Where do people use private browsing?



Obviously, the vast majority of the respondents use private browsing at home (77.7%). What is more surprising is that only 36.3% of the people who use private browsing use it in a public place. It might be that they never use a public computer, or it might be another symptom of people misunderstanding what they are protected from. This misunderstanding also likely contributes to the high usage of private browsing at work (22%), despite its ineffectiveness for hiding browsing patterns from network administrators. Another potential factor in the use of private browsing at work is separating personal browsing from work browsing.

Private browsing is an important feature that is used by over 20% of the Internet population. Unfortunately, many people use it for the wrong reasons, and this can be harmful, as it gives them a false sense of security. In recent years, Firefox and Opera have added features to mitigate web tracking to meet users' demand. This is a very strong departure from the previous common stance, which was not to block stateless tracking, as it is almost impossible to do so perfectly. While this new direction benefits users by offering them more choices, it also increases the need to raise awareness about privacy-enhancing technology so that users can make informed choices.

A big thanks to Aleksandra Korolova (http://theory.stanford.edu/~korolova/) and Ben Livshits (https://www.doc.ic.ac.uk/~livshits/) who helped shape this blog post.

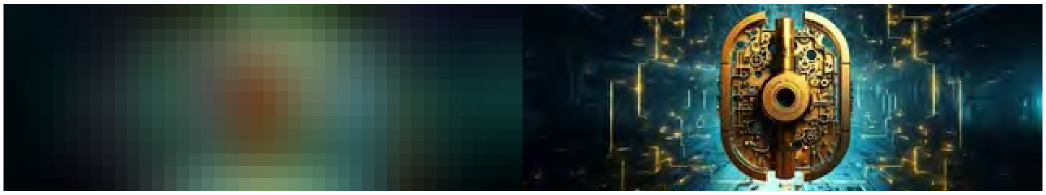
Thank you for reading this post till the end! If you enjoyed it, please don't forget to share it on your favorite social network so that your friends and colleagues can enjoy it too and learn how to use private browsing.

To get notified when the next post is online, follow me on Twitter (/)(https://twitter.com/elie), Facebook (https://www.facebook.com/elieblog), LinkedIn (https://www.linkedin.com/in/bursztein/). You can also get the full posts directly in your inbox by subscribing to the mailing list or my RSS feed (http://feeds.feedburner.com/inftoint).

web security (/tag/web-security/) survey (/tag/survey/)

Recent

BLOG POSTS
PUBLICATIONS
TALKS



CRYPTOGRAPHY

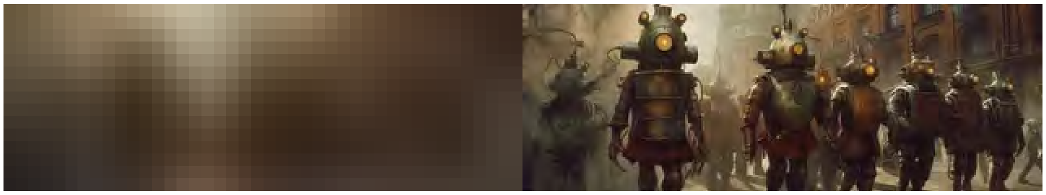
Hybrid Post-Quantum Signatures in Hardware Security Keys

Hybrid Post-Quantum Signatures in Hardware Security Keys

We introduce a hybrid digital signature scheme based on two building blocks: a classically-secure scheme, ECDSA, and a post-quantum secure one, Dilithium. Our hybrid scheme maintains the guarantees of each underlying building block even if the other one is broken, thus being resistant to classical and quantum attacks.

ACNS 2023

(/publication/hybrid-post-quantum-signatures-in-hardware-security-keys/)



AI

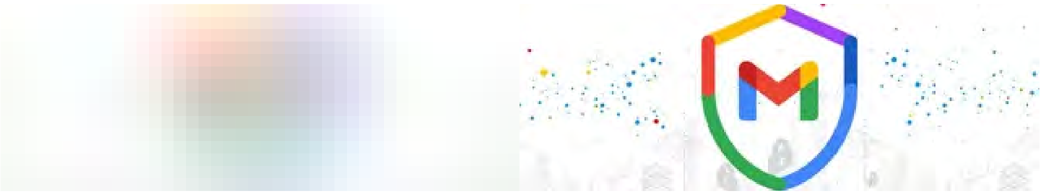
On the consequences of the AI workforce entering the market

On the consequences of the AI workforce entering the market

(/blog/ai/on-the-consequences-of-ai-workforce-entering-the-market/)

Exploring the societal impact of the GenAI workforce entering the market.

Jun 2023



CYBERSECURITY

How AI helps keeping Gmail inboxes malware free

How AI helps keeping Gmail inboxes malware free

(/talk/how-ai-helps-keeping-gmail-inboxes-malware-free/)

This talk provides an overview of how Google uses AI to strengthen Gmail's document defenses and withstand attacks that evade traditional AVs

FIC 2023

ELiE
(https://elie.net)

Elie Bursztein, leader of Google's anti-abuse research team, which invents transformative security and anti-abuse solutions that help protect users against online threats.

HOME (/)
TALKS (/TALKS/)
ABOUT (/ABOUT/)

PUBLICATIONS (/PUBLICATIONS
BLOG (/BLOG/)
NEWSLETTER

(https://www.twitter.com/elie)

(https://www.facebook.com/eliel

(https://github.com/ebursztein)

(https://www.youtube.com/c/ebu

(https://www.linkedin.com/in/bu

(https://www.instagram.com/elie

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #391

A Study on Private Browsing: Consumer Usage, Knowledge, and Thoughts

January 2017

Table of Contents

Introduction

At DuckDuckGo, our vision is to raise the standard of trust online. To that end, we strive to understand what people know about online privacy and how they use the privacy features available to them. This report focuses on the feature in web browsers commonly referred to as “Private Browsing.”

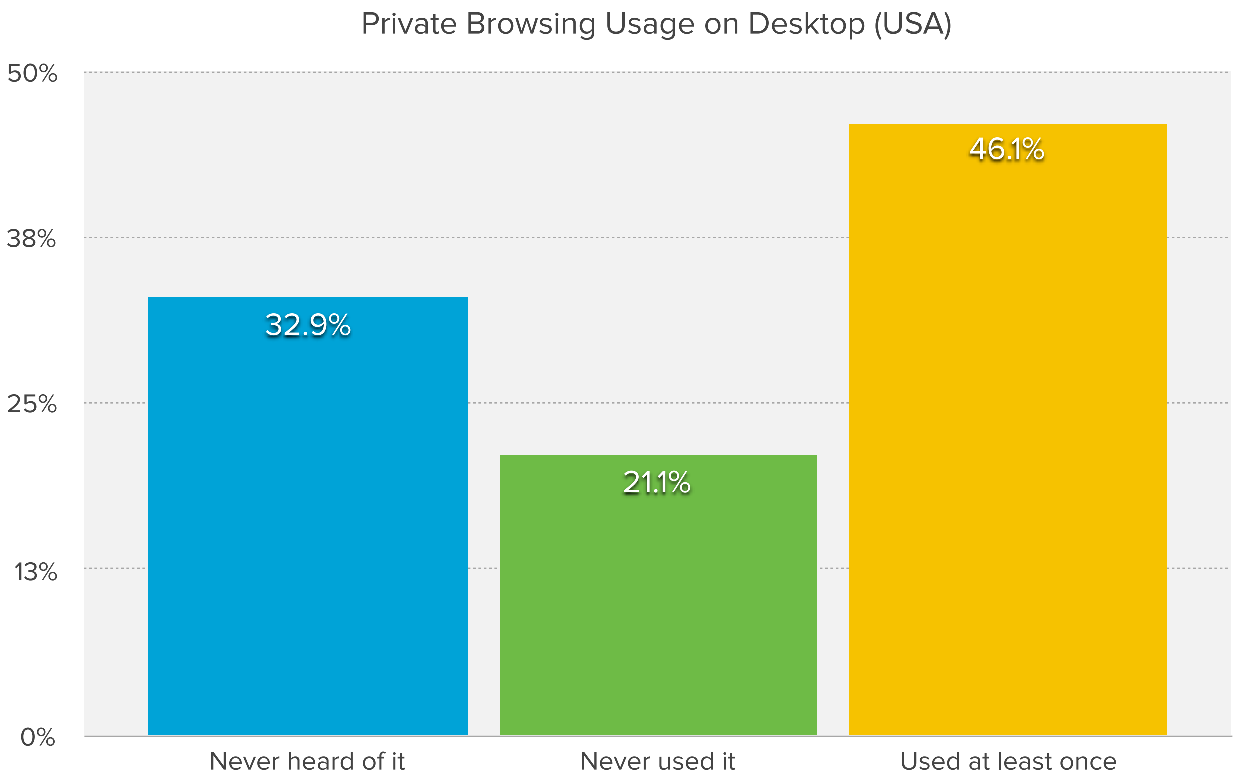
“Private Browsing,” “Privacy Mode,” “Secret Mode,” or “Incognito Mode” is a system of web browsing that clears browsing history and file cache after use. Despite Private Browsing being one of the most commonly known and used privacy features, we find that most people misunderstand the privacy protections it provides.

Our findings are based on a survey conducted with a random sampling of 5,710 Americans who were asked to share their experiences with Private Browsing.

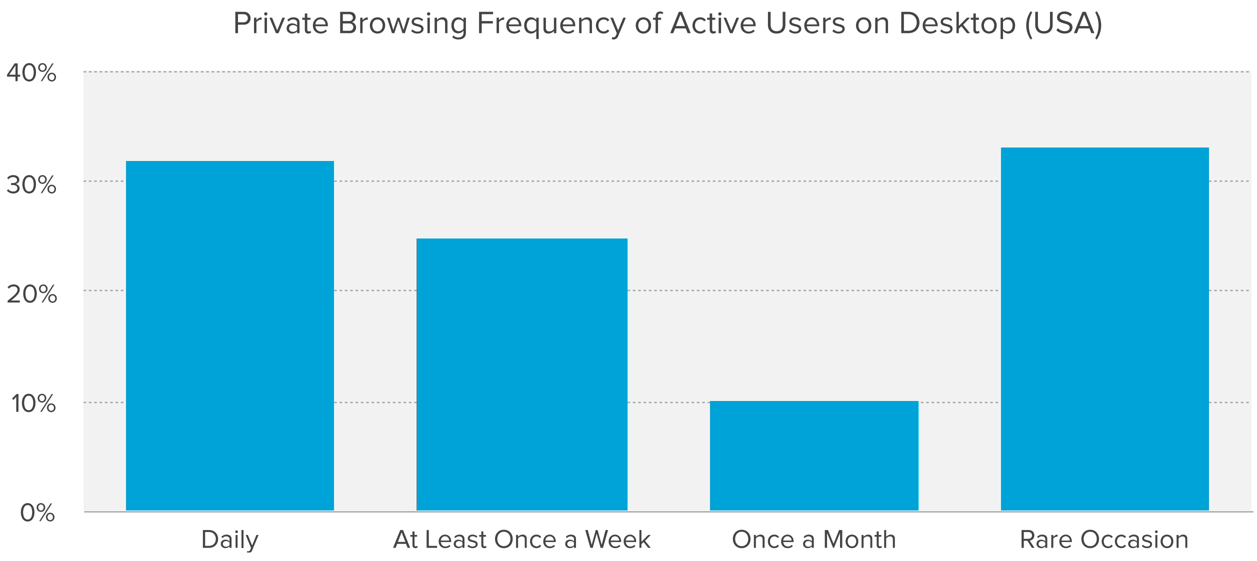
How Do People Use Private Browsing?

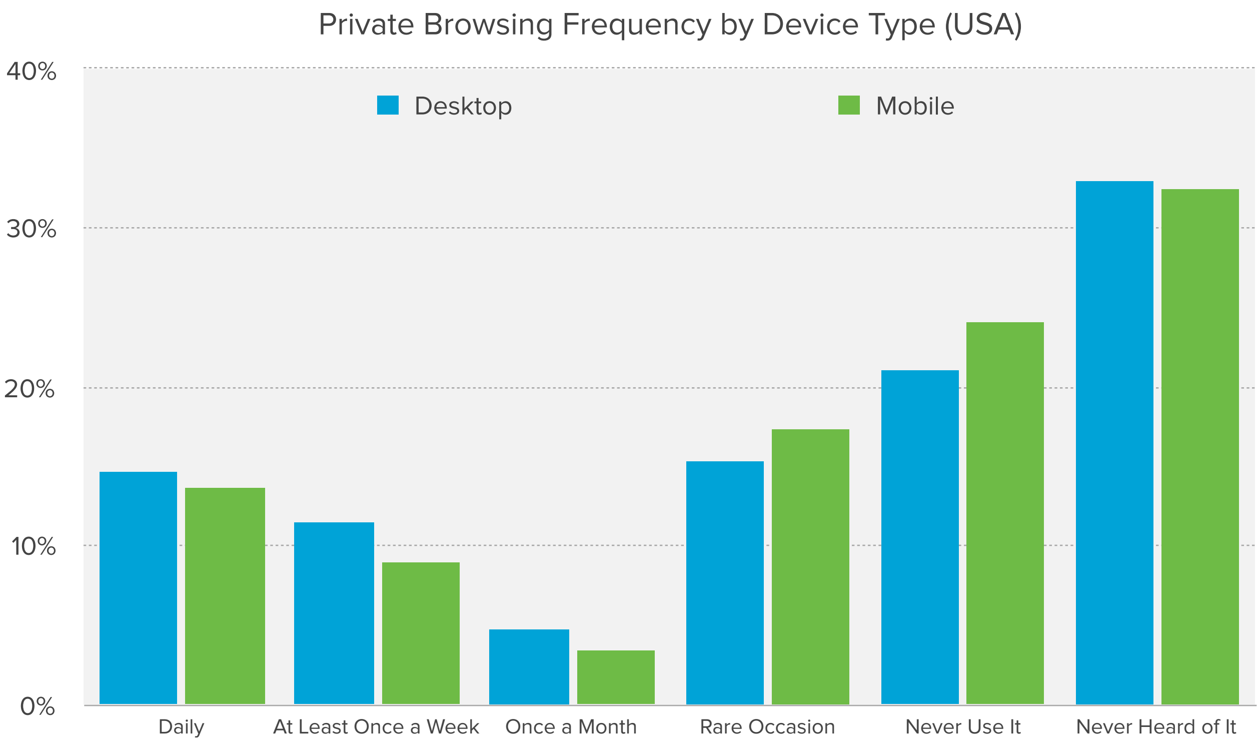
46% of Americans have used Private Browsing.

On desktop, we found that 46.1 ±1.7% of people have used a *"Private Browsing Mode"* at least once, and on mobile that number is 43.5 ±2.7%.

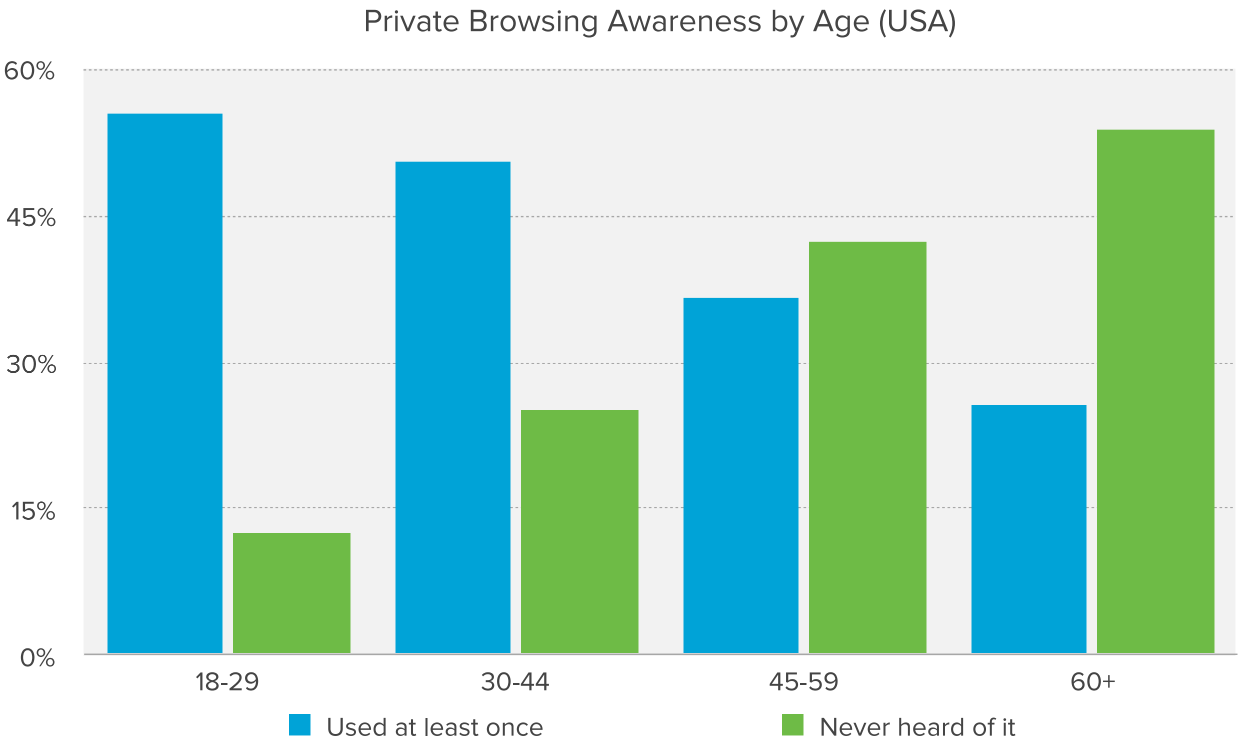


Of those who have used Private Browsing on desktop, 32.9 ±2.3% report using it “*Daily*,” while another 24.8 ± 2.1% report using it “*At Least Once a Week*.” On mobile, 31.5 ±3.9% report “*Daily*” usage, while another 20.6 ±3.3% report usage of “*At Least Once a Week*.”





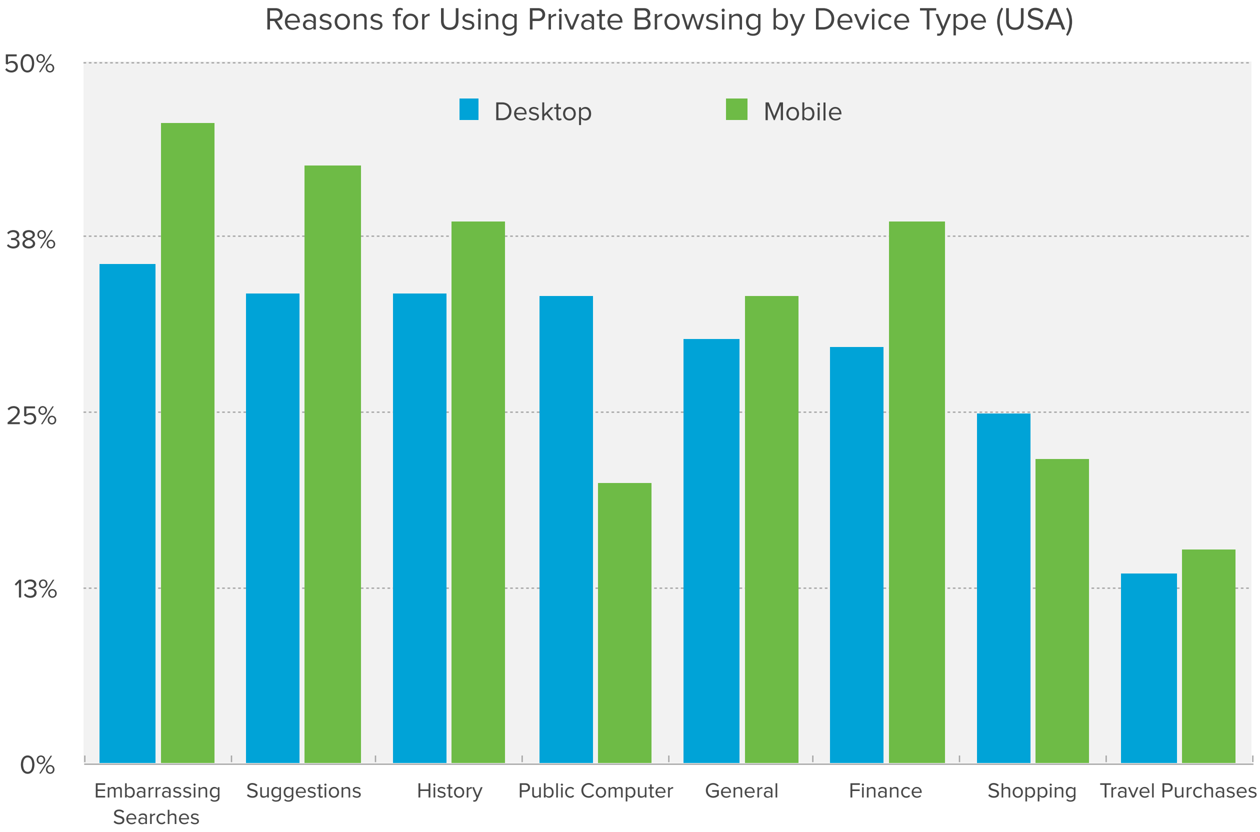
Younger people (18-29) are five times more likely to have heard of Private Browsing than older people (60+), but only twice as likely to have used it. This suggests that older audiences, while less likely to know about Private Browsing, adopt it more frequently once they hear about it.



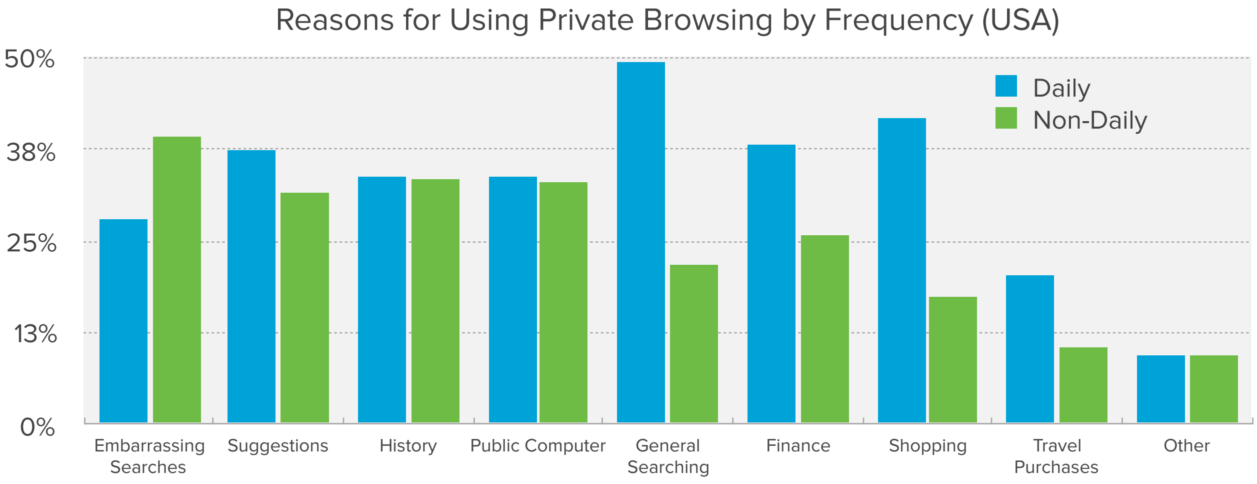
Why Do People Use Private Browsing?

The number one reason people use Private Browsing is "Embarrassing Searches."

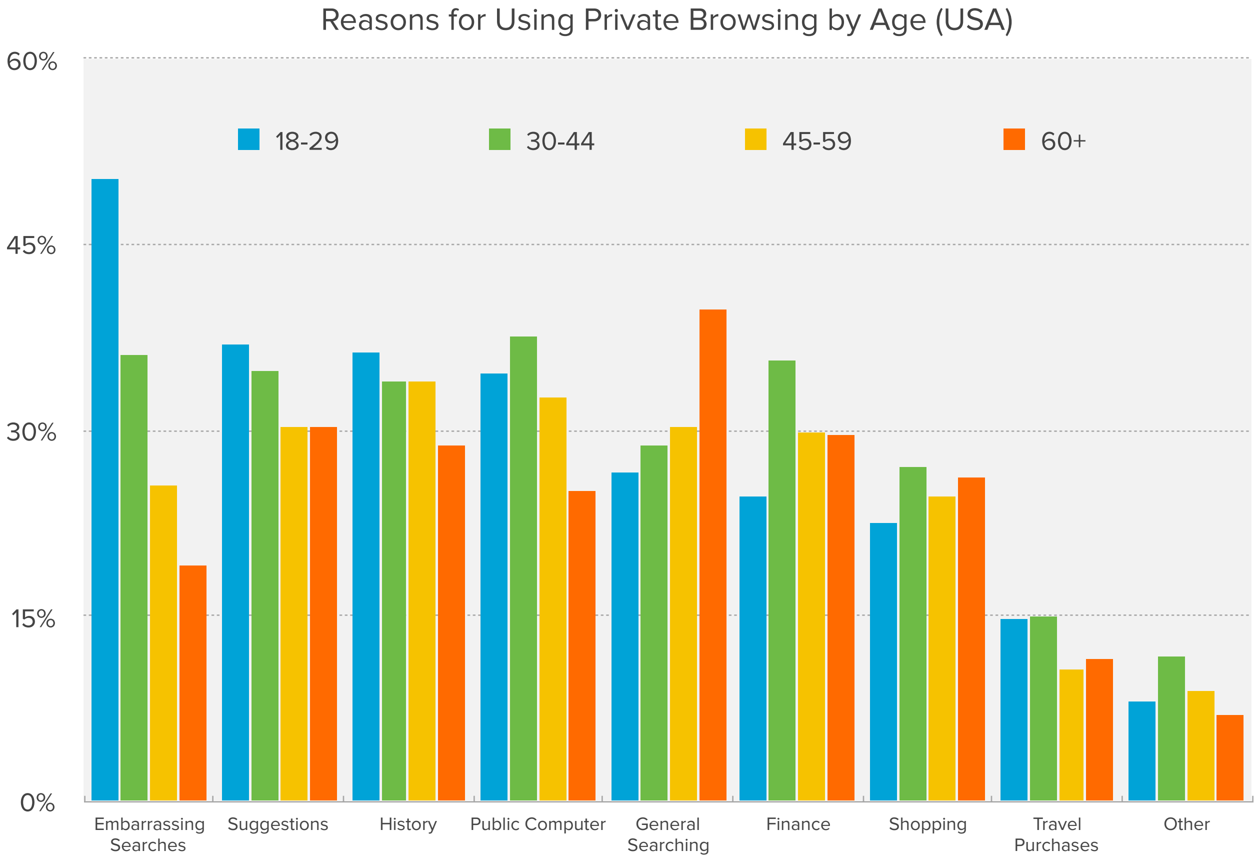
The number one reason people use private browsing is "*Embarrassing Searches*," at 35.7 ±2.5%. Other reasons fell between 24.9 ±2.2% and 33.5 ±2.4%, excluding "*Travel Purchases*," and "*Other*."



People who use Private Browsing daily are two times as likely to use it for "*General Searching*" and about two and half times more likely to use it for "*Shopping*" than non-daily users.



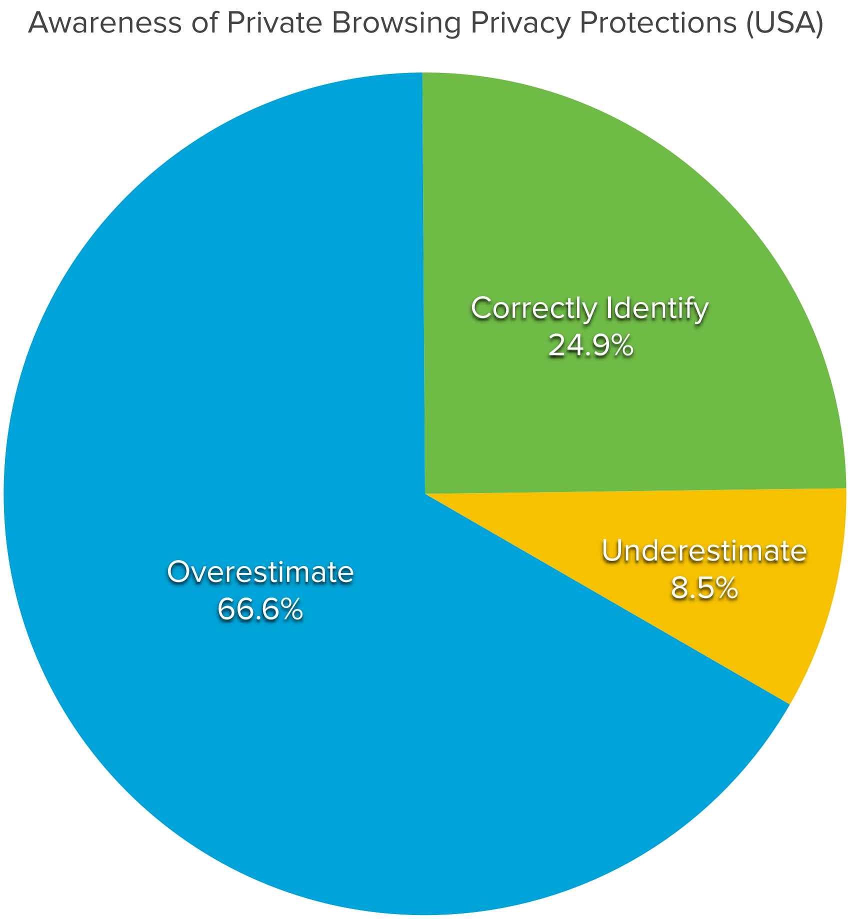
While most reasons for using Private Browsing remain consistent across age brackets, "*Embarrassing Searches*" goes down with age while "*General Searching*" goes up.



What Do People Know About Private Browsing?

76% of Americans who use Private Browsing mode cannot accurately identify the privacy benefit it provides.

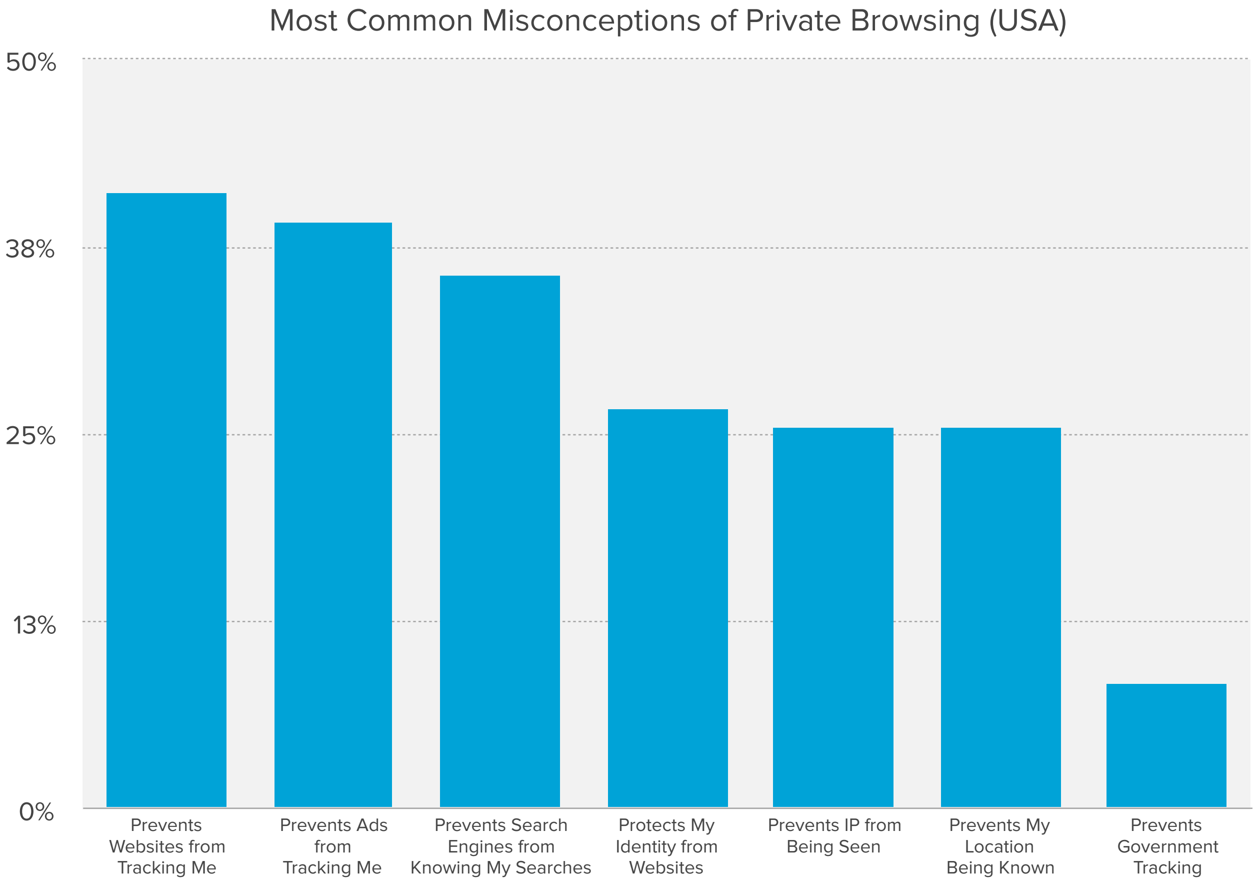
75.8 ±2.2% of people who use Private Browsing mode cannot accurately identify the privacy benefit it provides. Of that group, 66.5 ±2.5% overestimate the protection that Private Browsing provides.



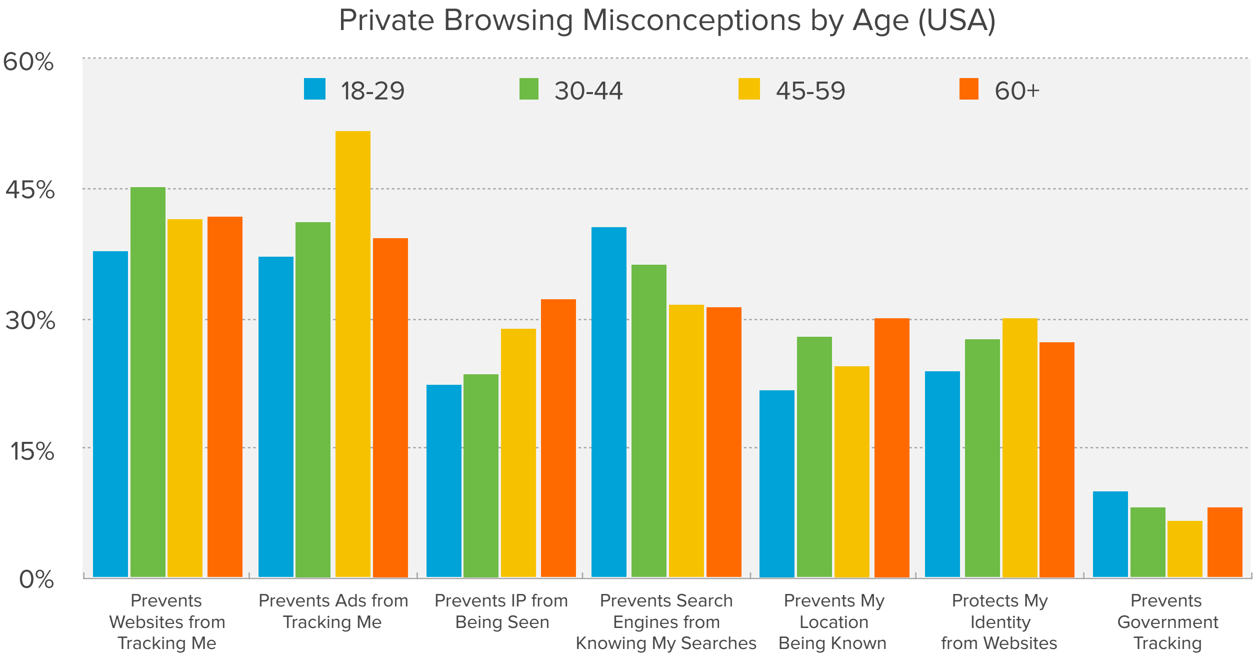
36% of Americans believe that Private Browsing mode prevents a search engine from knowing their searches.

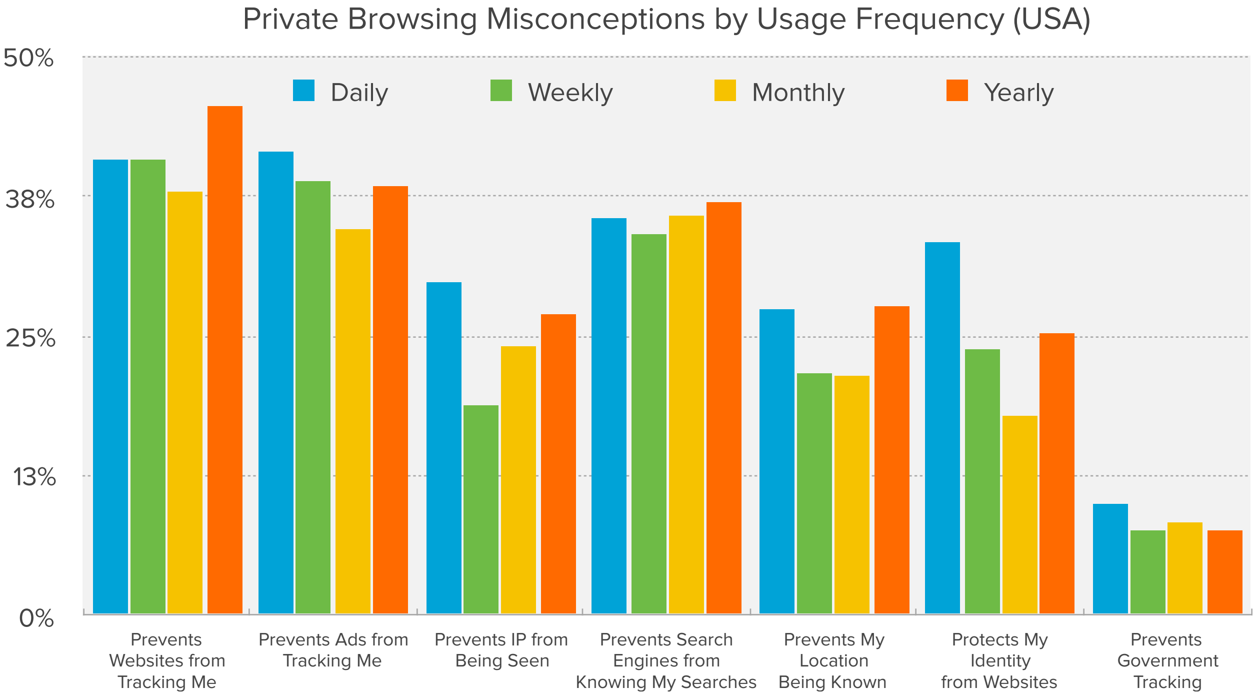
The top 3 misconceptions are:

- 41.0 ±2.5% believe that Private Browsing "*Prevents websites from tracking me*."
- 39.1 ±2.6% believe that Private Browsing "*Prevents ads from tracking me*."
- 35.7 ±2.5% believe that Private Browsing "*Prevents search engines from knowing my searches*."



For the most part, the misconceptions about Private Browsing are consistent. However, younger audiences are more likely to believe a search engine couldn't see their searches in Private Browsing mode, whereas older audiences are more likely to believe that Private Browsing mode would protect their IP address from being seen.



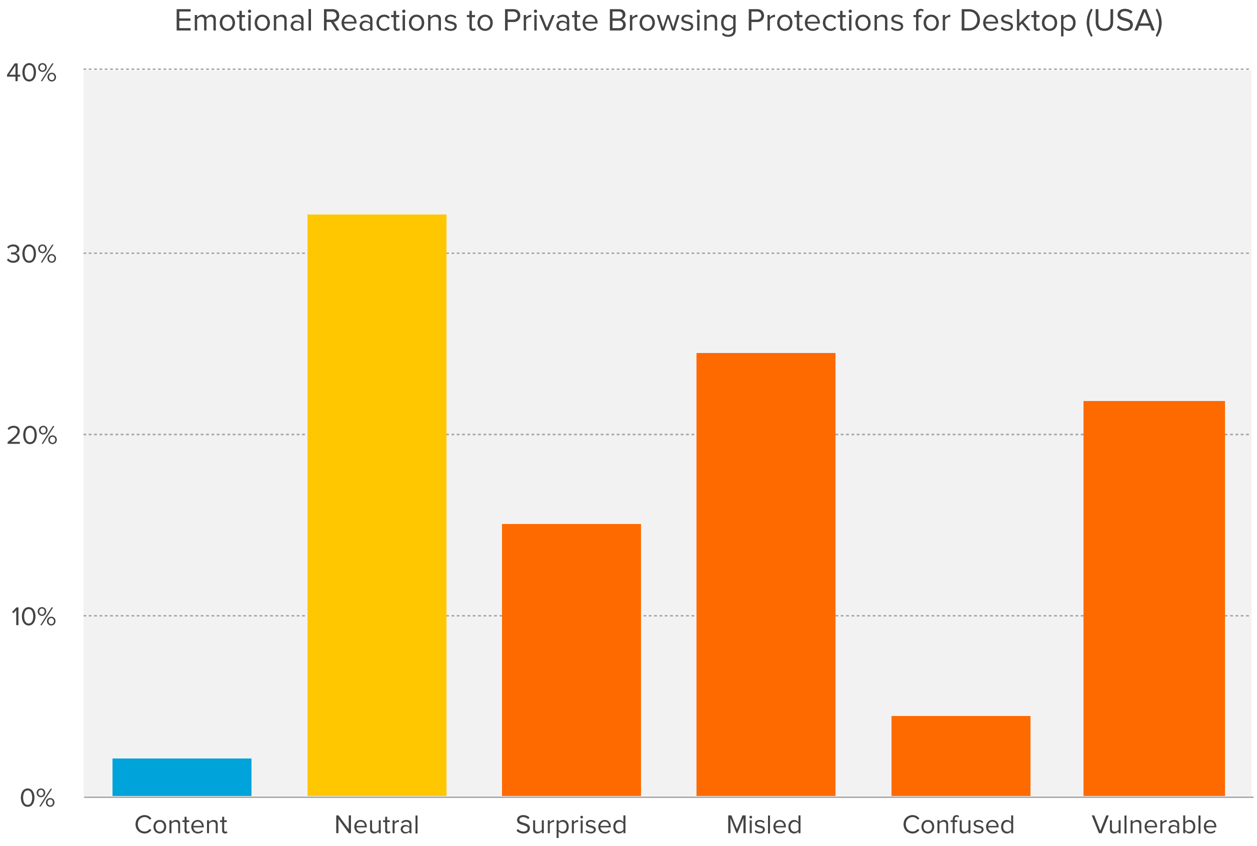


How Do Consumers React to Private Browsing Knowledge?

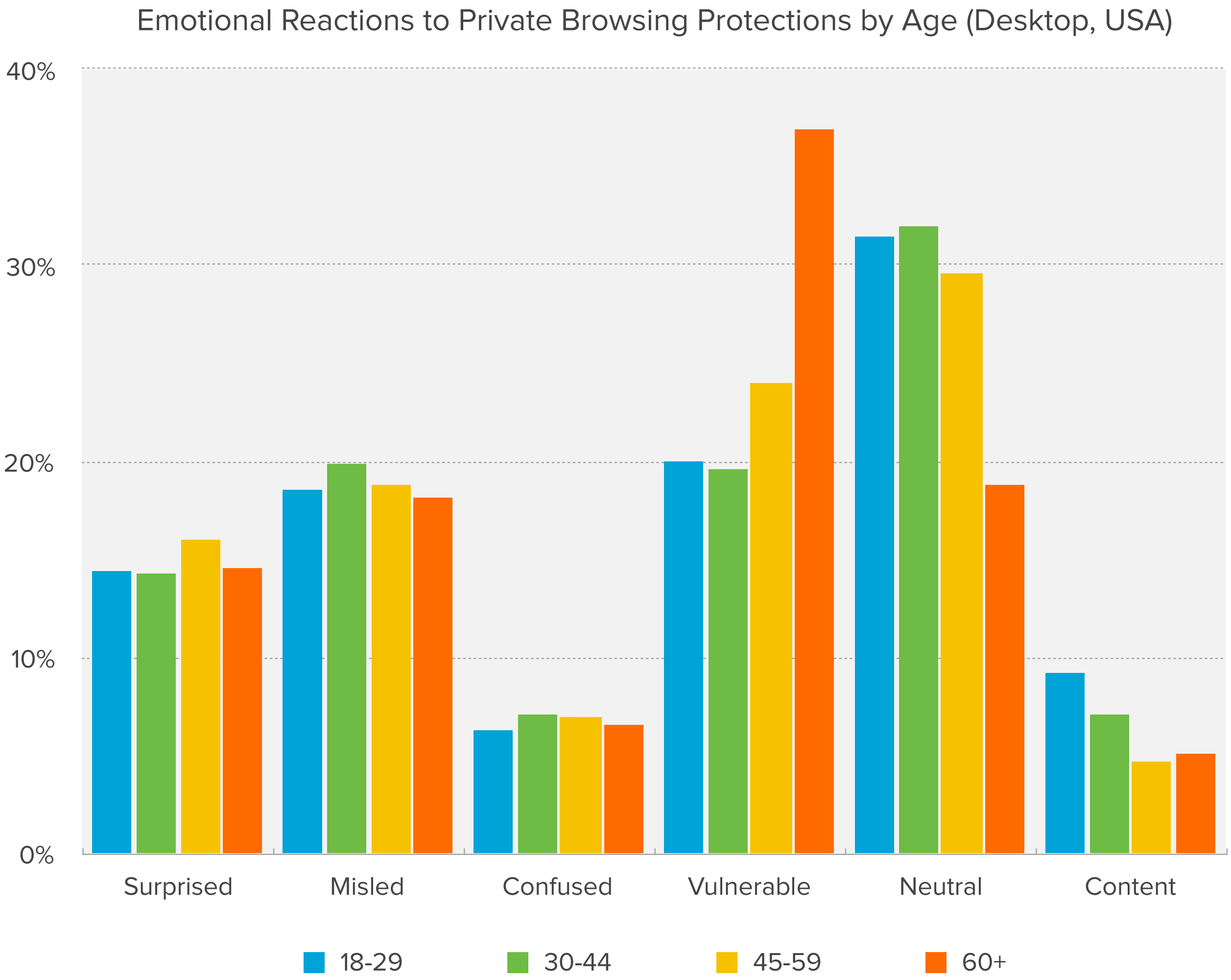
After asking about Private Browsing usage and knowledge, we informed people about what privacy protections Private Browsing provides, and asked about their emotional reaction:

> *Private Browsing mode only prevents your browser history from being recorded on your computer and does not offer any additional protection such as preventing the websites you visit from collecting your information (e.g. your searches on a search engine). How does that make you feel?*

Of the 75.8 ±2.2% of people who have misconceptions about private browsing protections, 65.9 ±2.4% feel "*Surprised*", "*Misled*", "*Confused*" or "*Vulnerable*" upon learning about its real protections.



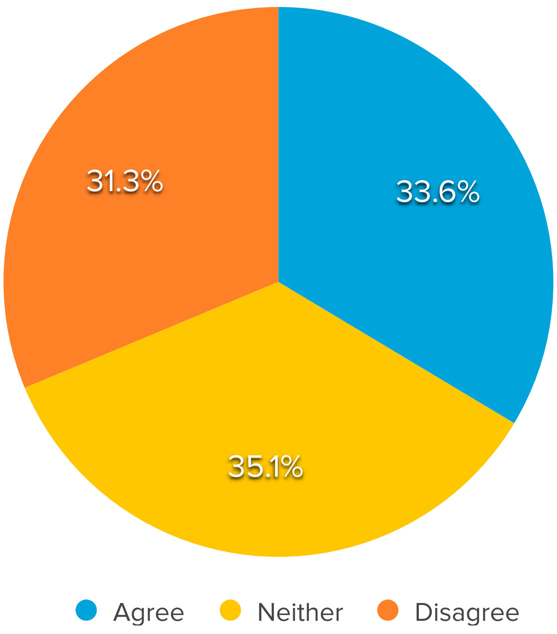
These emotional reactions span age. One notable difference is that 32.1 ±6.4% of people over 60 feel “*Vulnerable*” upon learning about Private Browsing’s limitations, vs less than 25% in other age groups.



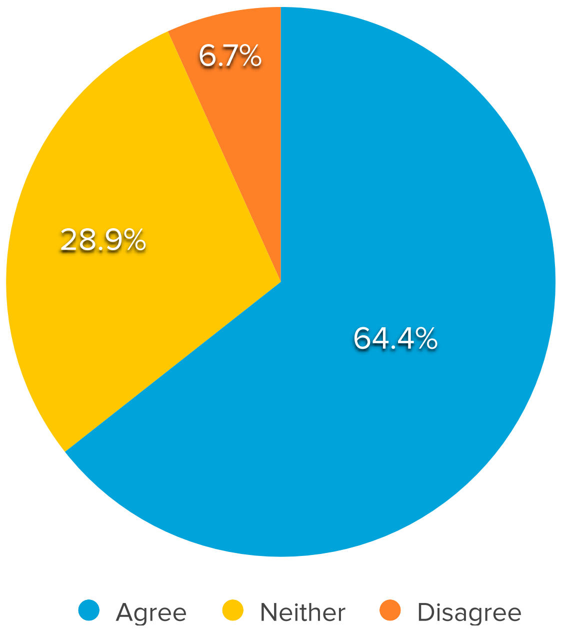
64% of Americans “Agree” or “Strongly Agree” with the statement “I wish my browser did more to protect my privacy.”

When then asked users to agree or disagree with the statement “*My browser does enough to protect my privacy,*” we found a rather even split. When further asked to agree or disagree with the statement “*I wish my browser did more to protect my privacy*,” users were much more strongly in favor of additional privacy protection.

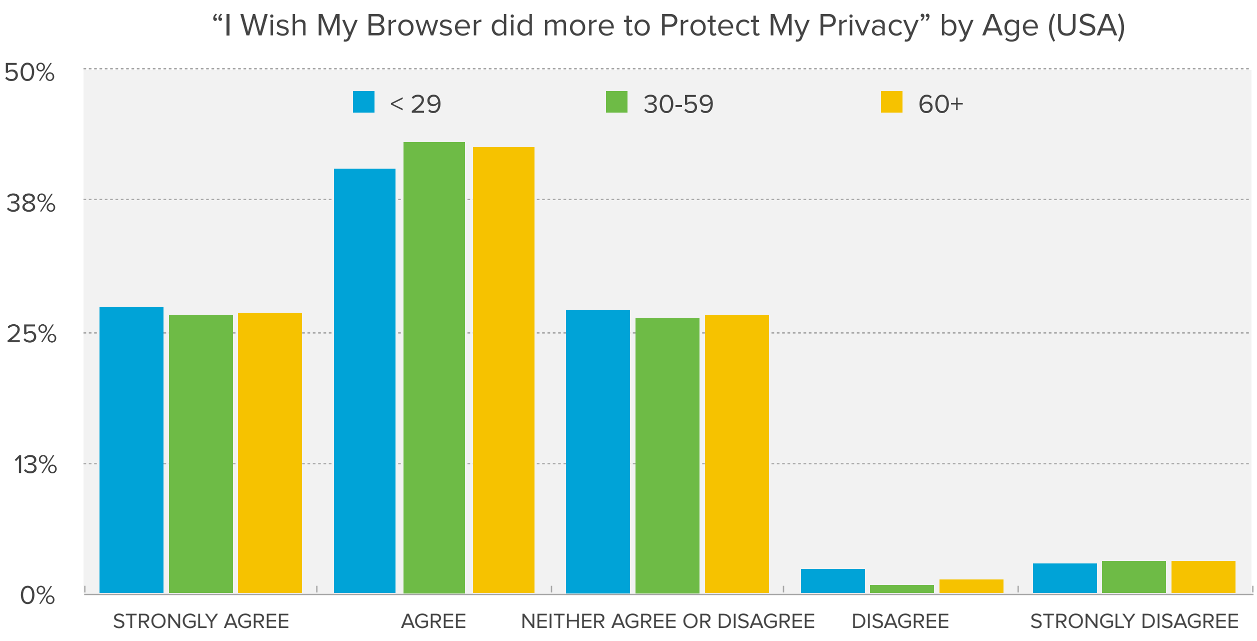
“My Browser Does Enough for Privacy” (USA)



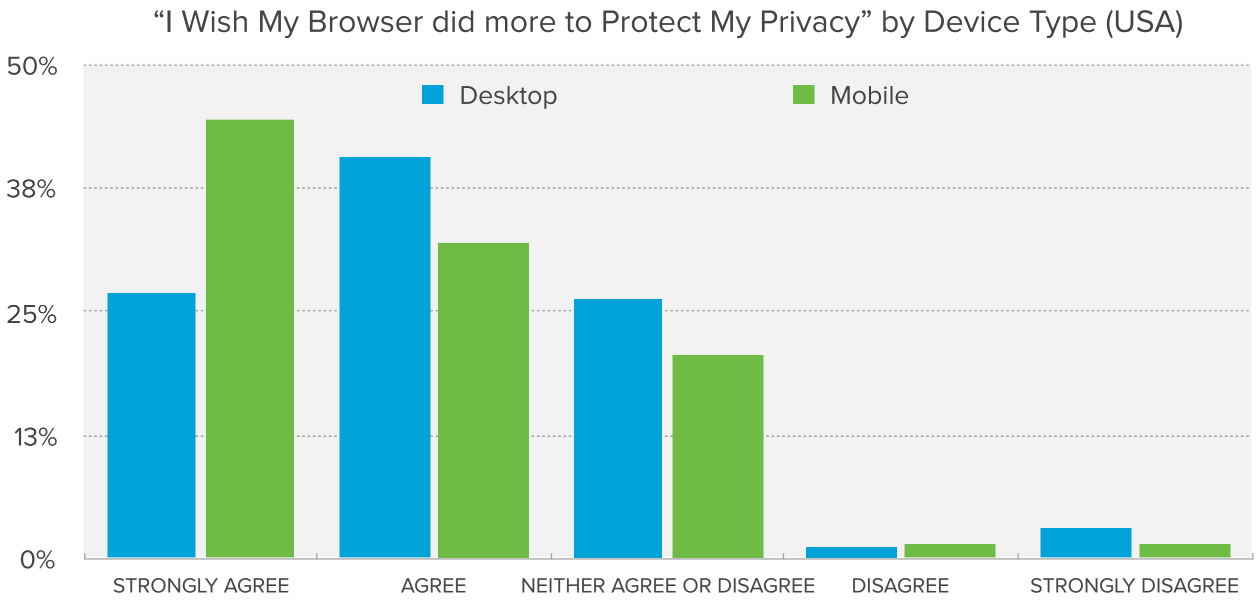
“I Wish My Browser Did More to Protect My Privacy” (USA)



Once again, these findings were consistent across every age group.



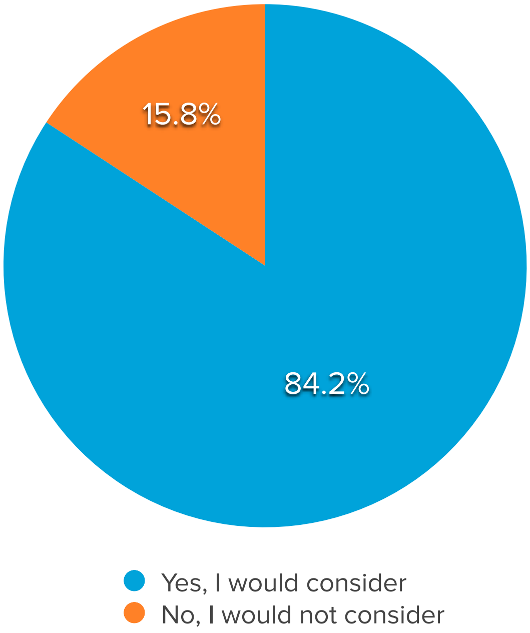
Though when comparing Desktop vs Mobile, we saw a slight skew with mobile users being more likely to “*Strongly Agree*” than *“Agree*.”



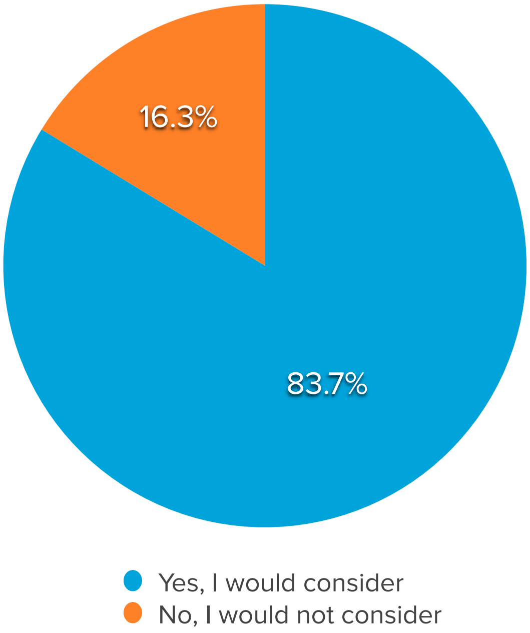
84% of Americans would consider trying another major web browser if it offered more features to help protect their privacy.

We found people willing to make major changes to better protect their privacy. 84.2 ±1.9% of people say they would "*consider trying another major web browser if it offered more features to help protect your privacy*," and 83.7 ±2.0% say they would "*consider trying another major web browser if it offered a Private Browsing mode that uses a search engine that didn't track your searches*."

"Would you consider trying another major browser if it offered additional privacy features?" (USA)



"Would you consider trying another major web browser if it had a private browsing mode that used a search engine that didn't track your searches?" (USA)



Key Takeaways about Private Browsing

1. With 46.1 ± 1.7% of American's having used Private Browsing at least once and 26.7 ±3.0% using it at least once a week, it is clear that Private Browsing is a popular privacy protecting feature.

2. However, 75.8 ±2.2% of people who use Private Browsing incorrectly identify the protection that it provides. As 66.5 ±2.5% overestimate its benefits, this leaves a majority of Private Browsing users exposed more than they think they are.

3. When people find out what private browsing actually does, 65.9 ±2.4% feel "*Surprised*", "*Misled*", "*Confused*" or "*Vulnerable*." 64.0 ±2.6% of people believe their web browser should do more to protect their privacy, and 84.2 ±1.9% are open to trying to a different major web browser if it would provide more privacy protection.

Methodology

These results are based on the polling of a random sample of 5,710 Americans via SurveyMonkey's "Audience" program that "ensures panelists are representative of the U.S. population." Heen, Lieberman and Miethe (2014) confirmed, "Depending on the purpose of the survey research, the average discrepancy rate of 5 to 10% between the particular demographic characteristics of online respondents and their known distribution in the U.S. population may or may not be problematic."[1]

During this survey, respondents reserved the right to decline to answer any survey question. This was allowed in order to prevent biasing answers in the event a user did not understand the question, felt uncomfortable answering the question, or felt there was no answer that accurately represented their response. In these cases of "item non-response," the sample population size was adjusted for that question. A respondent who did not complete all the questions still had their responses included in questions they did complete. The only exception are statements made in this survey that required responses from more than one question.

Respondents were compensated for participation in this survey.

[1] http://www.unlv.edu/sites/default/files/page_files/27/ComparisonDifferentOnlineSampling.pdf

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #423

NEW YORK POST

LOG IN

RECOMMENDED

NASA sending spacecraft on 7-year journey to metal…

TECH

Google’s incognito mode isn’t as private as you thought

By Sean Keach, The Sun

Published Aug. 22, 2018
Updated Aug. 22, 2018, 1:14 p.m. ET

ORIGINALLY PUBLISHED BY:

Google’s Incognito Mode is a great way to hide your online antics — but there’s a big hole that could leave you exposed.

A new study from Vanderbilt University reveals a sneaky way Google can see exactly what you’ve been looking at online.

THE Sun

'Ring of Fire' hit with 70 earthquakes in just 48 hours

Facebook to rate users on trustworthiness

World's biggest plane set for the skies

NASA admits Opportunity rover could be lose forever

The study investigated how Google collects info from across devices (like Android or Chromebooks) and services (like Google, YouTube and the Chrome web browser).

And it revealed something very surprising about Incognito Mode.

It emerged that Google can still record the websites you browse while in Incognito Mode on the Chrome browser and link them to your identity.

This will come as a surprise to some users who thought the special setting protected them.

Incognito Mode is a setting on Chrome that prevents your web history from being stored.

It also won't store cookies — small files about you — that are linked to your identity.

If you're logged into Google, much of what you do online can be traced back to your personal account.

But if you switch Incognito Mode on, you'll only receive "anonymous" cookies and Google won't be able to link your identity to your browsing habits.

Sadly, there's a catch.

If you log back into Google before leaving Incognito Mode, Google will be able to retroactively link your browsing data to your account.

That means Google could see information from before you logged in, but while you were in Incognito Mode — and link it to your Google identity.

This works by taking the previously anonymous cookies and then associating them with your Google account.

The only way to get around this would be to only log into your Google account after you've left Incognito Mode.

"While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user's personal credentials stored in their Google Account," the study explained.

Before you go ...

Before you go ...

Before you go ...

Before you go ...

Before you go ...

Before you go ...

Before you go ...

Before you go ...

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #447

Overview

Published on Monday, March 28, 2016

Table of contents ▾

Chrome DevTools is a set of web developer tools built directly into the [Google Chrome](#) browser. DevTools can help you edit pages on-the-fly and diagnose problems quickly, which ultimately helps you build better websites, faster.

```
      };
      const value = () => Math.floor(Math.
      const r = value();
      const g = value();
      const b = value();
      return {r, g, b};
    };
    debugger;
    const target = document.querySelector(
    const color = rgb();
    target.style.color = `rgb(${color.r},
    colors.push(color);
    debugger;
  });
 });
</script>
</section>
<section id="breakpoints">
```

Check out the video for live demonstrations of core DevTools workflows, including debugging

There are many ways to open DevTools, because different users want quick access to different parts of the DevTools UI.

To work with the DOM or CSS, right-click an element on the page and select **Inspect** to jump into the **Elements** panel. Or press `Command+Option+C` (Mac) or `Control+Shift+C` (Windows, Linux, ChromeOS).

To see logged messages or run JavaScript, press `Command+Option+J` (Mac) or `Control+Shift+J` (Windows, Linux, ChromeOS) to jump straight into the **Console** panel.

See Open Chrome DevTools for more details and workflows.

Get started

If you're a more experienced web developer, here are the recommended starting points for learning how DevTools can improve your productivity:

View and change the DOM

View and change CSS

Debug JavaScript

View messages and run JavaScript in the Console

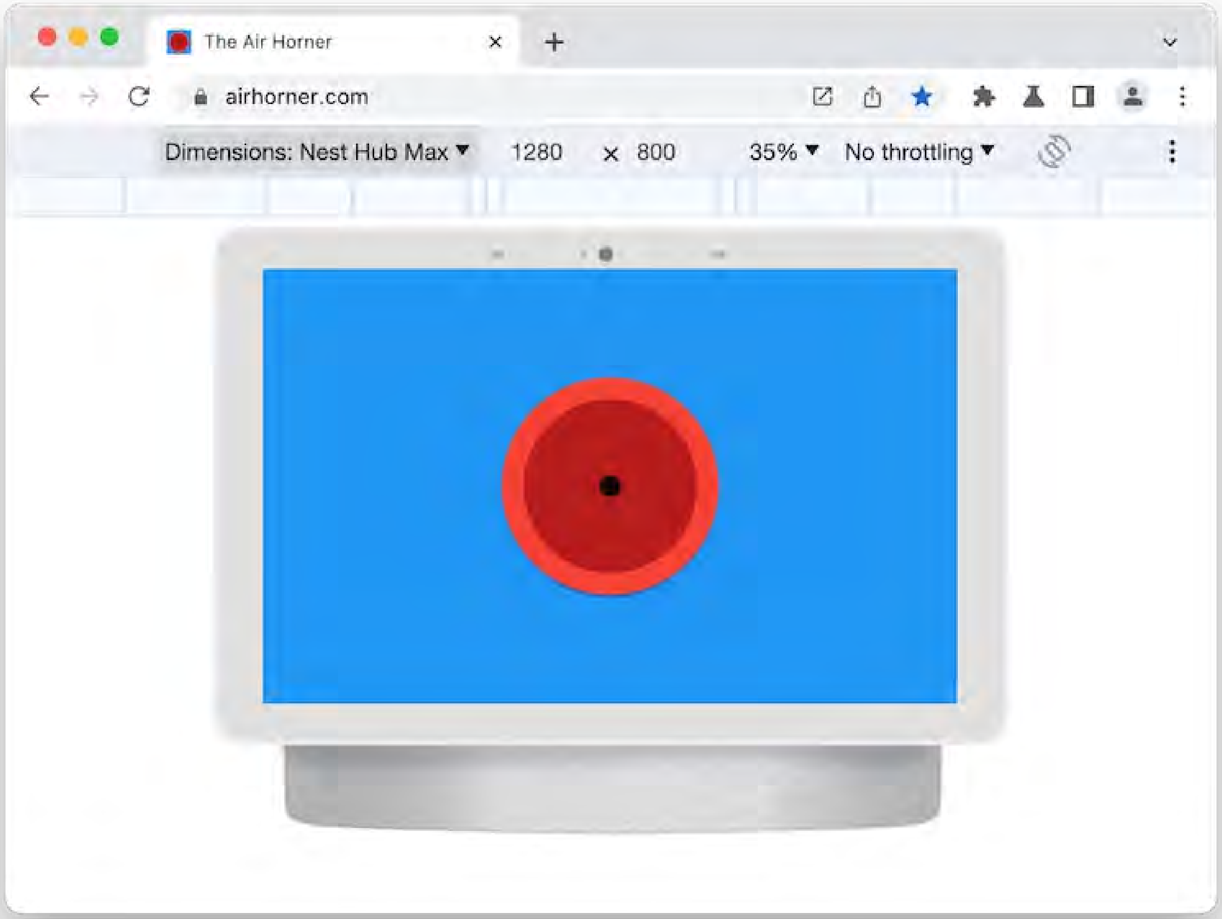
Optimize website speed

Inspect network activity

Discover DevTools

The DevTools UI can be a little overwhelming... there are so many tabs! But, if you take some time to get familiar with each tab to understand what's possible, you may discover that DevTools can

Device Mode



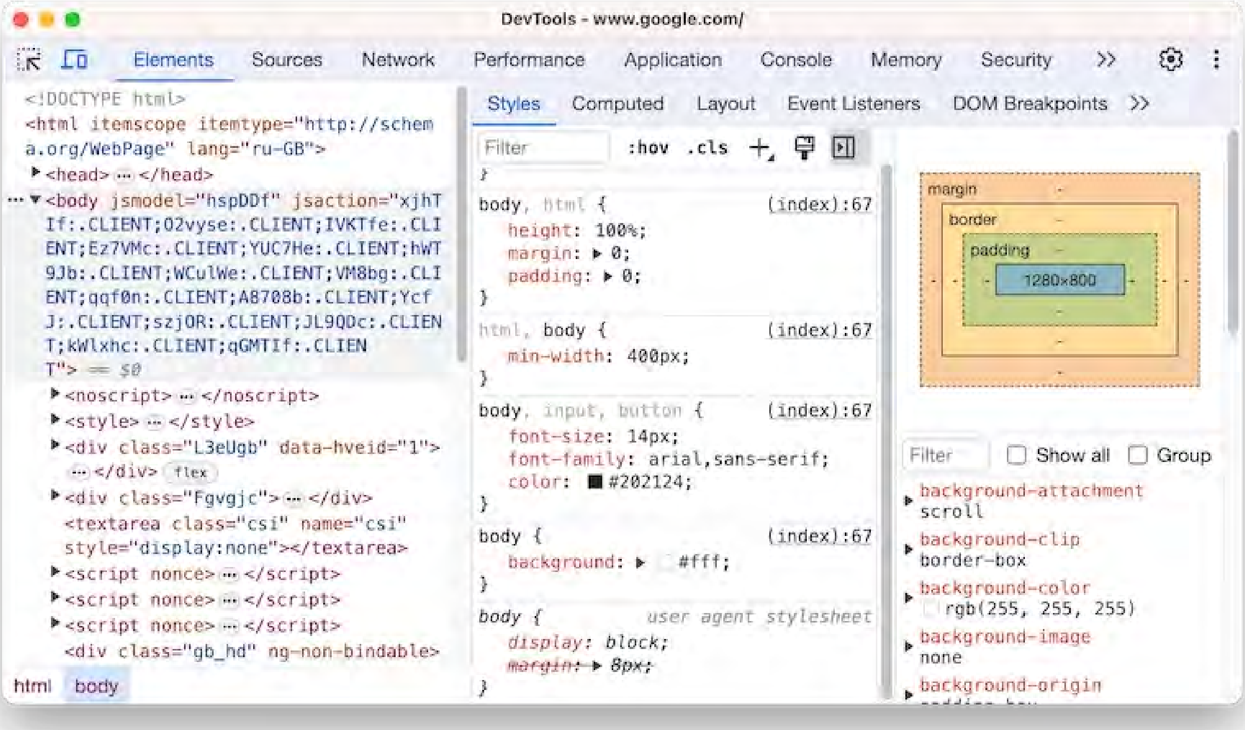
Simulate mobile devices.

[Device mode](#)

[Emulate device sensors](#)

Elements panel

This site uses cookies to deliver and enhance the quality of its services and to analyze traffic. If you agree, cookies are also used to serve advertising and to personalize the content and advertisements that you see. Learn more about our use of cookies.



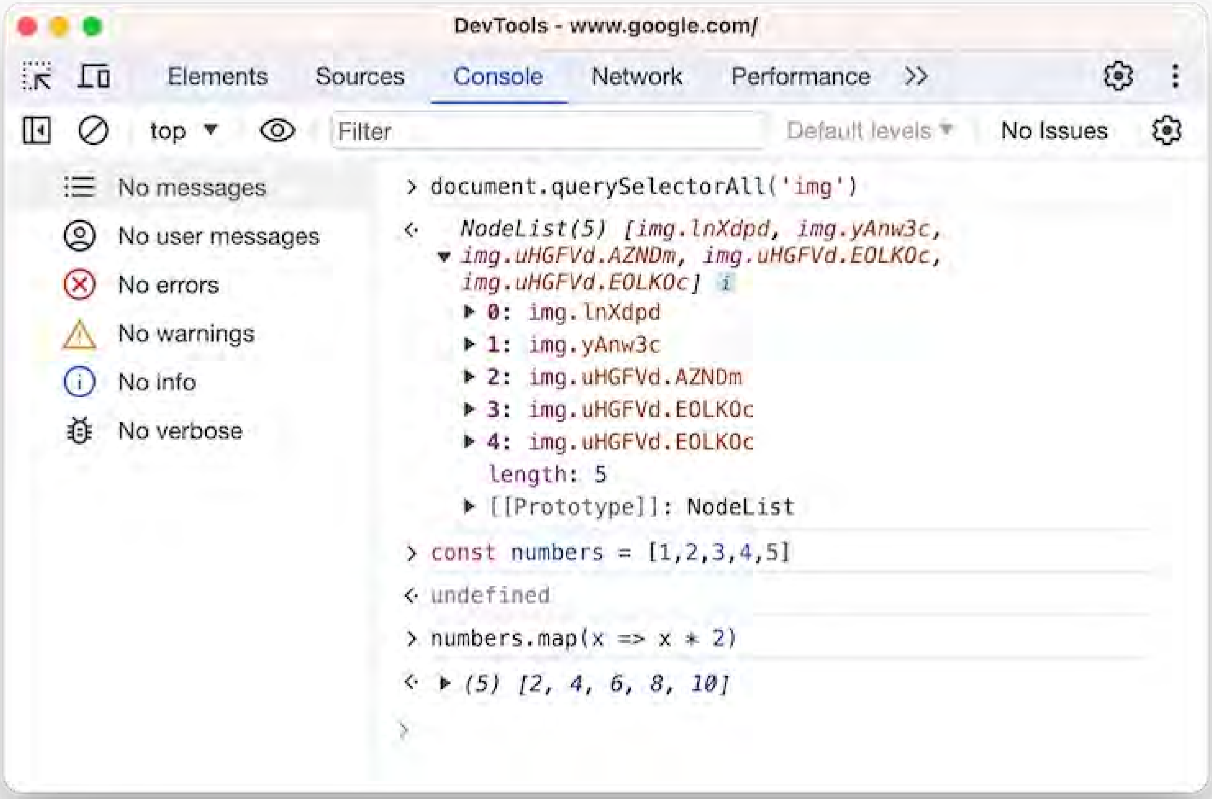
```
<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/WebPage" lang="ru-GB">
 ▶<head> … </head>
… ▼<body jsmodel="hspDDf" jsaction="xjhTIf:.CLIENT;O2vyse:.CLIENT;IVKTfe:.CLIENT;Ez7VMc:.CLIENT;YUC7He:.CLIENT;hWT9Jb:.CLIENT;WCulWe:.CLIENT;VM8bg:.CLIENT;qqf0n:.CLIENT;A8708b:.CLIENT;YcfJ:.CLIENT;szjOR:.CLIENT;JL9QDc:.CLIENT;kWlxhc:.CLIENT;qGMTIf:.CLIENT"> == $0
   ▶<noscript> … </noscript>
   ▶<style> … </style>
   ▶<div class="L3eUgb" data-hveid="1"> … </div> flex
   ▶<div class="Fgvgjc"> … </div>
    <textarea class="csi" name="csi" style="display:none"></textarea>
   ▶<script nonce> … </script>
   ▶<script nonce> … </script>
   ▶<script nonce> … </script>
    <div class="gb_hd" ng-non-bindable>
```

```
}
body, html {                    (index):67
   height: 100%;
   margin: ▶ 0;
   padding: ▶ 0;
}
html, body {                    (index):67
   min-width: 400px;
}
body, input, button {           (index):67
   font-size: 14px;
   font-family: arial,sans-serif;
   color: ■ #202124;
}
body {                          (index):67
   background: ▶ □ #fff;
}
body {             user agent stylesheet
   display: block;
   ~~margin: ▶ 8px;~~
}
```

```
▶ background-attachment
  scroll
▶ background-clip
  border-box
▶ background-color
  □ rgb(255, 255, 255)
▶ background-image
  none
▶ background-origin
```

View and change the DOM and CSS.

- [Get started with viewing and changing the DOM]
- [Get started with viewing and changing CSS]
- [Edit CSS]
- [Edit the DOM]
- [Find invalid, overridden, inactive, and other CSS]
- [Identify potential CSS improvements]
- [Emulate light/dark themes, contrast, and other CSS media features]
- [Find unused CSS]
- [Inspect animations]

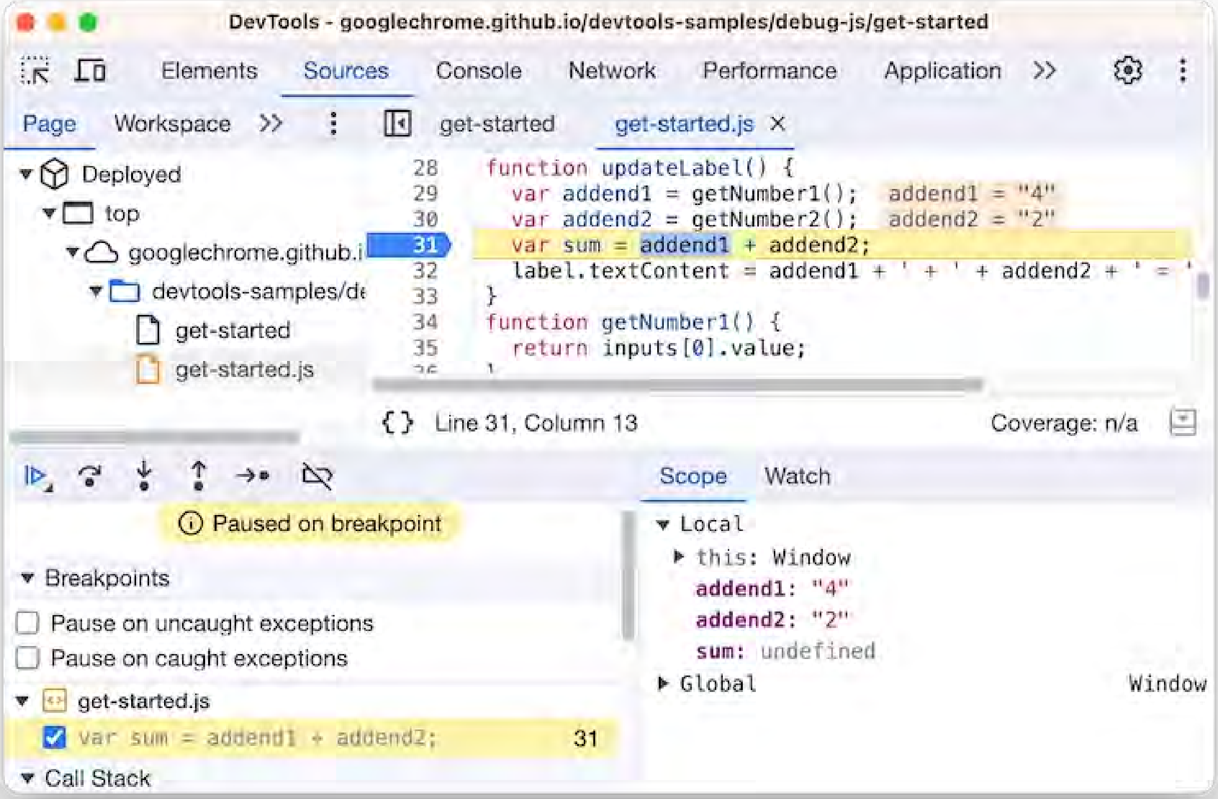


```
> document.querySelectorAll('img')
<  NodeList(5) [img.lnXdpd, img.yAnw3c,
 ▾ img.uHGFVd.AZNDm, img.uHGFVd.EOLKOc,
   img.uHGFVd.EOLKOc] i
     ▶ 0: img.lnXdpd
     ▶ 1: img.yAnw3c
     ▶ 2: img.uHGFVd.AZNDm
     ▶ 3: img.uHGFVd.EOLKOc
     ▶ 4: img.uHGFVd.EOLKOc
       length: 5
     ▶ [[Prototype]]: NodeList
> const numbers = [1,2,3,4,5]
< undefined
> numbers.map(x => x * 2)
< ▶ (5) [2, 4, 6, 8, 10]
>
```

View messages and run JavaScript from the Console.

- Get started with the Console
- Console Utilities API reference
- Console API reference

Sources panel



```
function updateLabel() {
  var addend1 = getNumber1();  addend1 = "4"
  var addend2 = getNumber2();  addend2 = "2"
  var sum = addend1 + addend2;
  label.textContent = addend1 + ' + ' + addend2 + ' = '
}
function getNumber1() {
  return inputs[0].value;
```

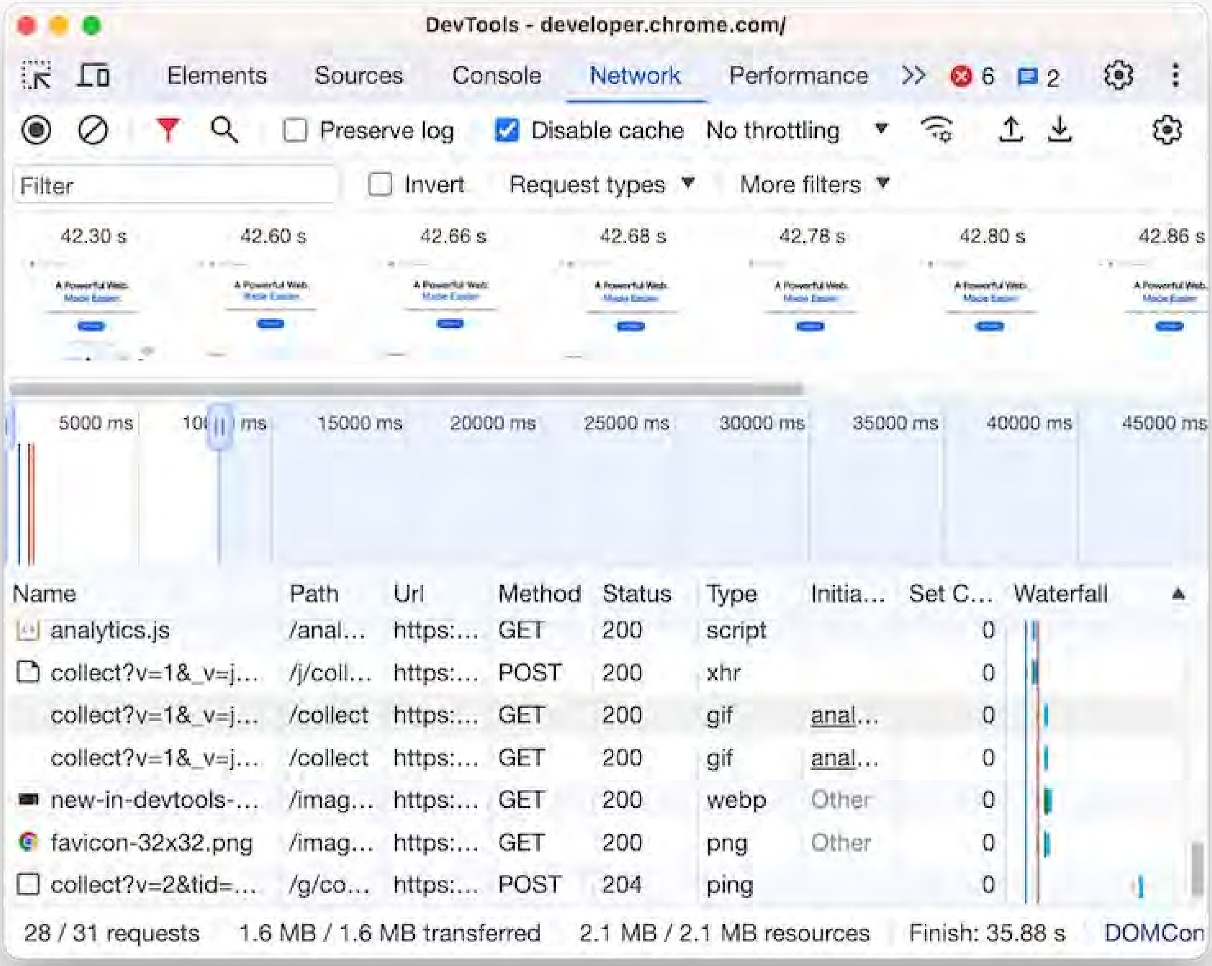
□ Pause on uncaught exceptions
□ Pause on caught exceptions

get-started.js
☑ var sum = addend1 + addend2; 31

```
▼ Local
  ▶ this: Window
    addend1: "4"
    addend2: "2"
    sum: undefined
▶ Global                Window
```

Debug JavaScript, persist changes made in DevTools across page reloads, save and run snippets of JavaScript, and save changes that you make in DevTools to local sources.

- Get started with debugging JavaScript
- Pause your code with breakpoints
- Edit and save files in a workspace
- Run snippets of JavaScript
- JavaScript debugging reference
- Override web content and HTTP response headers locally



☐ Preserve log ☑ Disable cache No throttling

☐ Invert

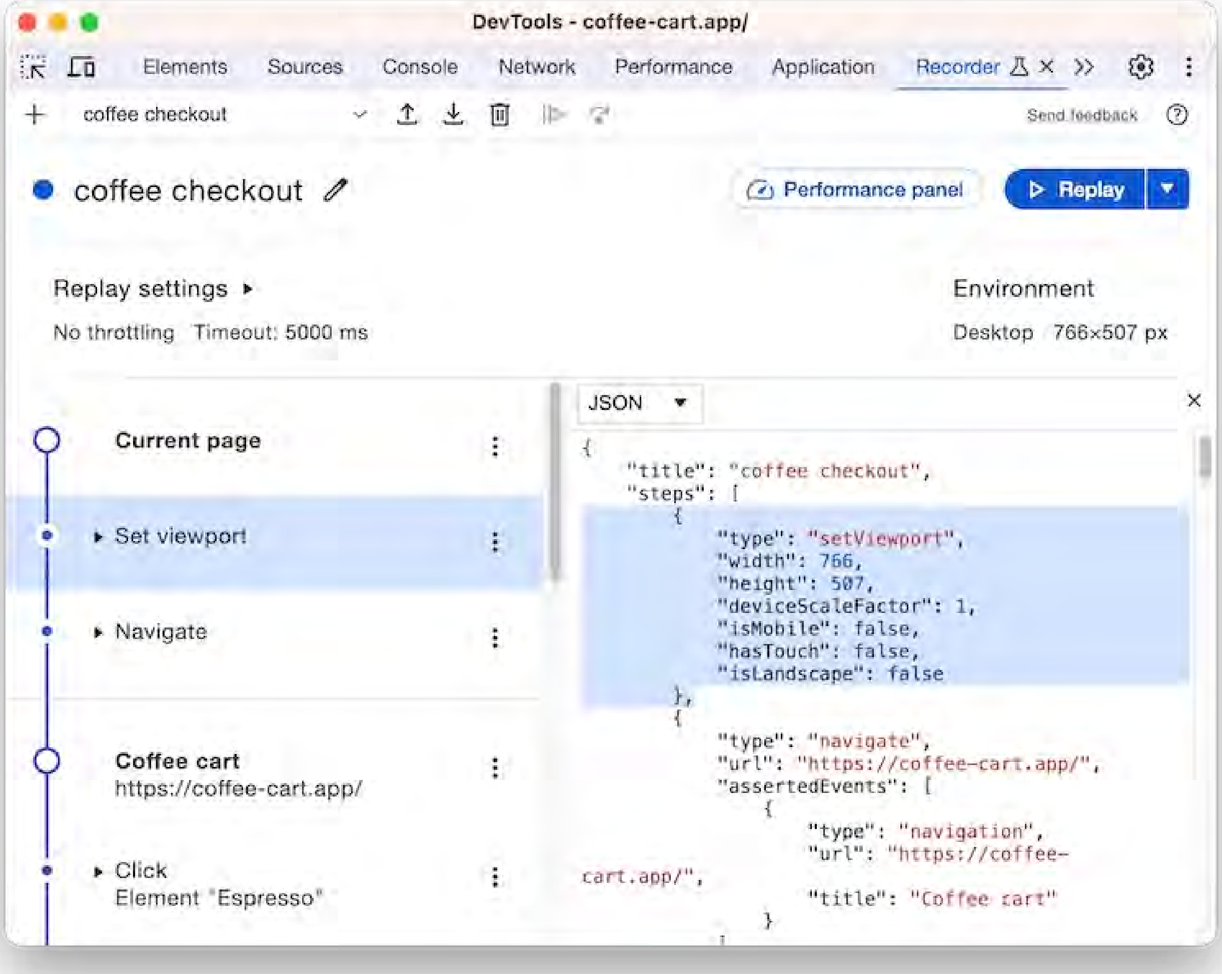
Name	Path	Url	Method	Status	Type	Initia…	Set C…	Waterfall
analytics.js	/anal…	https:…	GET	200	script		0	
collect?v=1&_v=j…	/j/coll…	https:…	POST	200	xhr		0	
collect?v=1&_v=j…	/collect	https:…	GET	200	gif	anal…	0	
collect?v=1&_v=j…	/collect	https:…	GET	200	gif	anal…	0	
new-in-devtools-…	/imag…	https:…	GET	200	webp	Other	0	
favicon-32x32.png	/imag…	https:…	GET	200	png	Other	0	
collect?v=2&tid=…	/g/co…	https:…	POST	204	ping		0	

28 / 31 requests 1.6 MB / 1.6 MB transferred 2.1 MB / 2.1 MB resources Finish: 35.88 s DOMCon

View and debug network activity.

- Inspect network activity
- Network features reference
- View page resources

Recorder panel



coffee checkout

Replay settings

No throttling Timeout: 5000 ms

Environment

Desktop 766×507 px

Current page

Set viewport

Navigate

Coffee cart
https://coffee-cart.app/

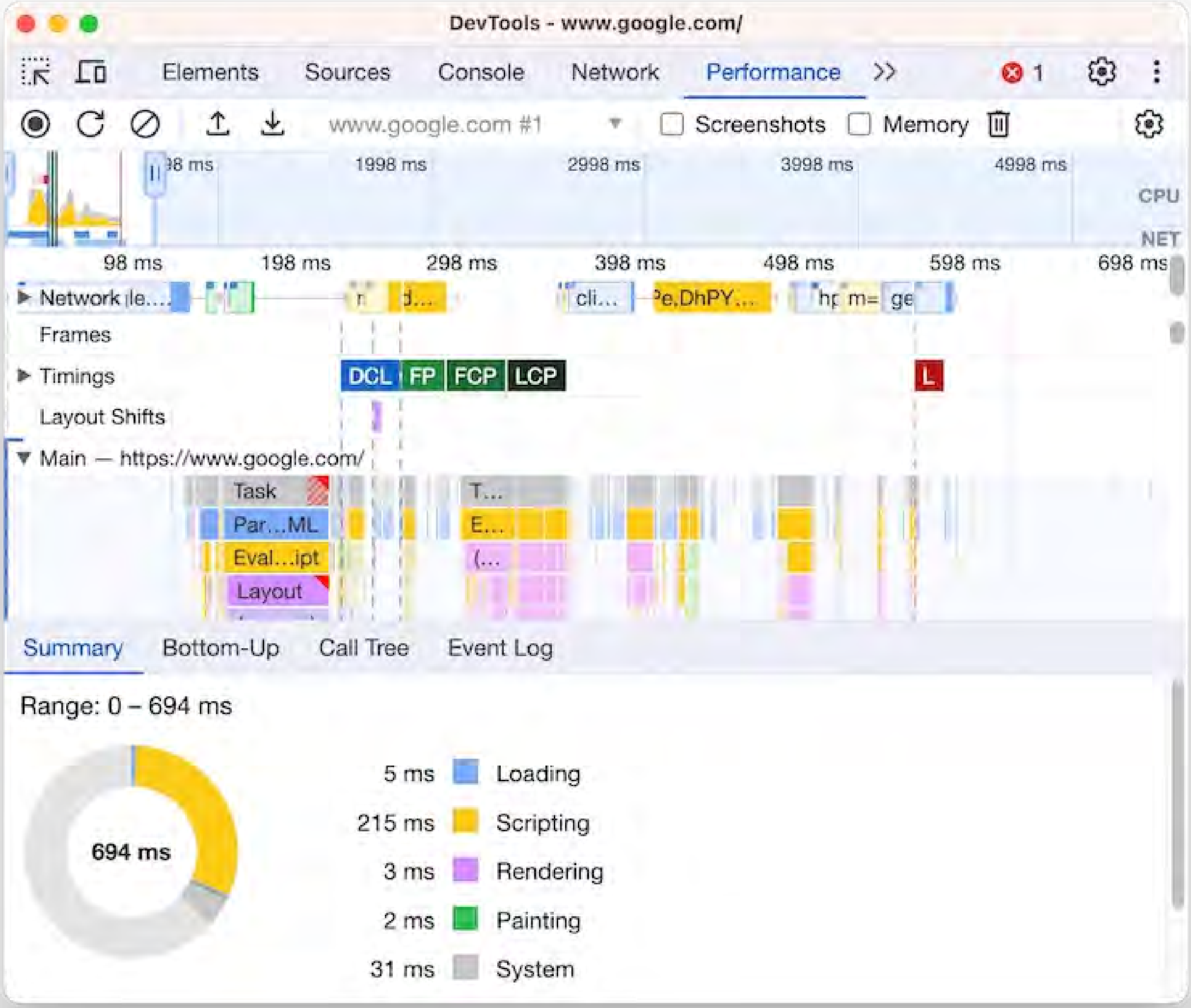
Click
Element "Espresso"

```
{
    "title": "coffee checkout",
    "steps": [
        {
            "type": "setViewport",
            "width": 766,
            "height": 507,
            "deviceScaleFactor": 1,
            "isMobile": false,
            "hasTouch": false,
            "isLandscape": false
        },
        {
            "type": "navigate",
            "url": "https://coffee-cart.app/",
            "assertedEvents": [
                {
                    "type": "navigation",
                    "url": "https://coffee-
cart.app/",
                    "title": "Coffee cart"
                }
```

Record, replay, and measure user flows.

- Record, replay, and measure user flows
- Customize the Recorder with extensions
- Recorder features reference

Performance panel



Range: 0 – 694 ms

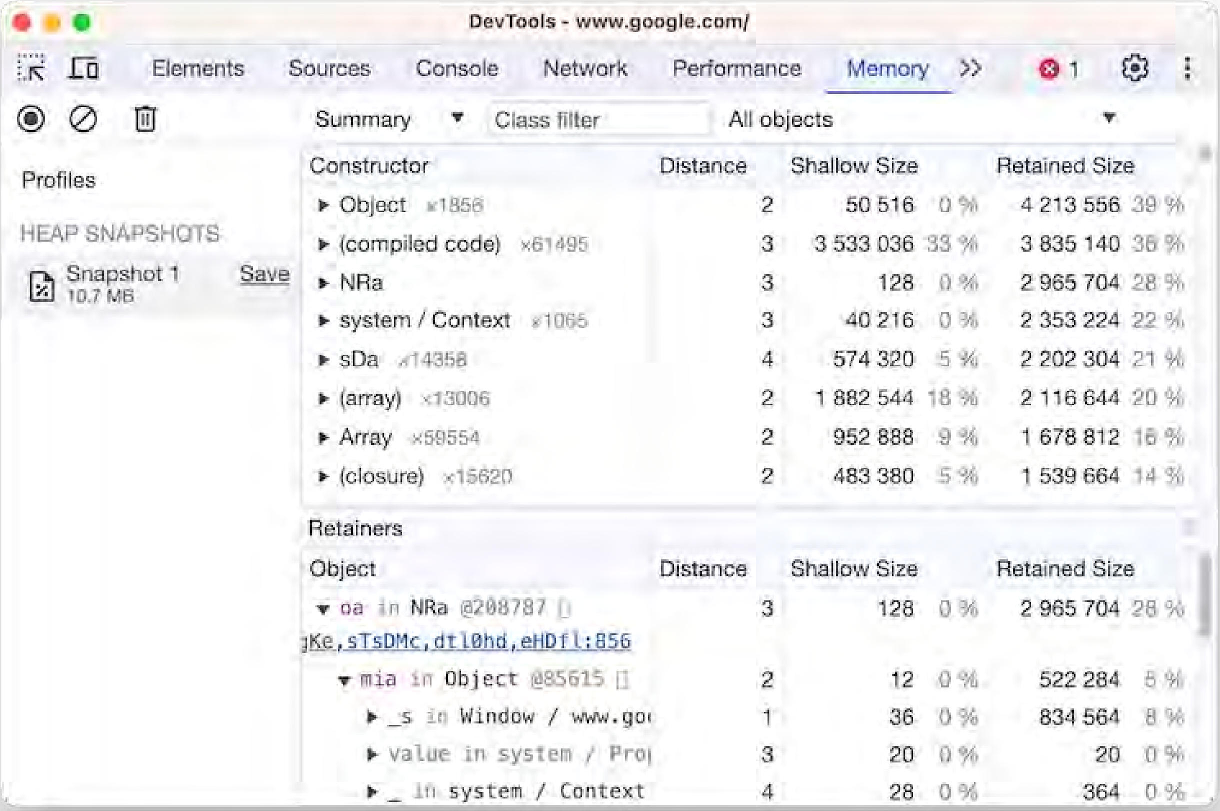
694 ms

5 ms 🟦 Loading
215 ms 🟨 Scripting
3 ms 🟪 Rendering
2 ms 🟩 Painting
31 ms ⬜ System

Find ways to improve load and runtime performance.

- Optimize website speed
- Analyze runtime performance
- Performance features reference

Memory panel



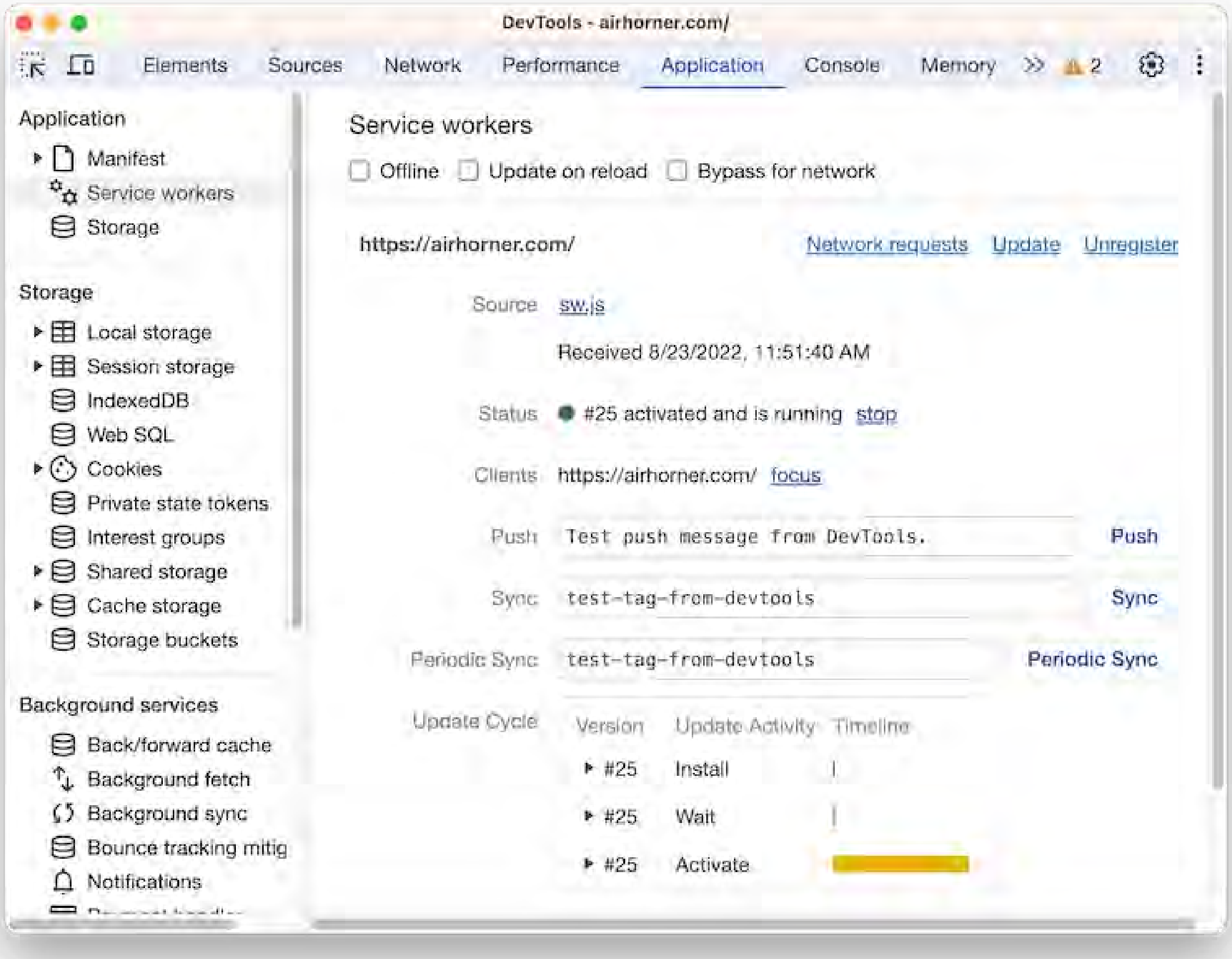
Constructor	Distance	Shallow Size		Retained Size	
▸ Object ×1856	2	50 516	0 %	4 213 556	39 %
▸ (compiled code) ×61495	3	3 533 036	33 %	3 835 140	36 %
▸ NRa	3	128	0 %	2 965 704	28 %
▸ system / Context ×1065	3	40 216	0 %	2 353 224	22 %
▸ sDa ×14358	4	574 320	5 %	2 202 304	21 %
▸ (array) ×13006	2	1 882 544	18 %	2 116 644	20 %
▸ Array ×59554	2	952 888	9 %	1 678 812	16 %
▸ (closure) ×15620	2	483 380	5 %	1 539 664	14 %

Object	Distance	Shallow Size		Retained Size	
▾ oa in NRa @208787 []	3	128	0 %	2 965 704	28 %
jKe,sTsDMc,dtl0hd,eHDfl:856					
▾ mia in Object @85615 []	2	12	0 %	522 284	5 %
▸ _s in Window / www.goo	1	36	0 %	834 564	8 %
▸ value in system / Pro	3	20	0 %	20	0 %
▸ _ in system / Context	4	28	0 %	364	0 %

Find and fix memory issues that affect page performance, for example, memory leaks.

Fix memory problems

Application panel



Service workers

□ Offline □ Update on reload □ Bypass for network

https://airhorner.com/

Source sw.js

Received 8/23/2022, 11:51:40 AM

Status ● #25 activated and is running

Clients https://airhorner.com/

Push Test push message from DevTools.

Sync test-tag-from-devtools

Periodic Sync test-tag-from-devtools

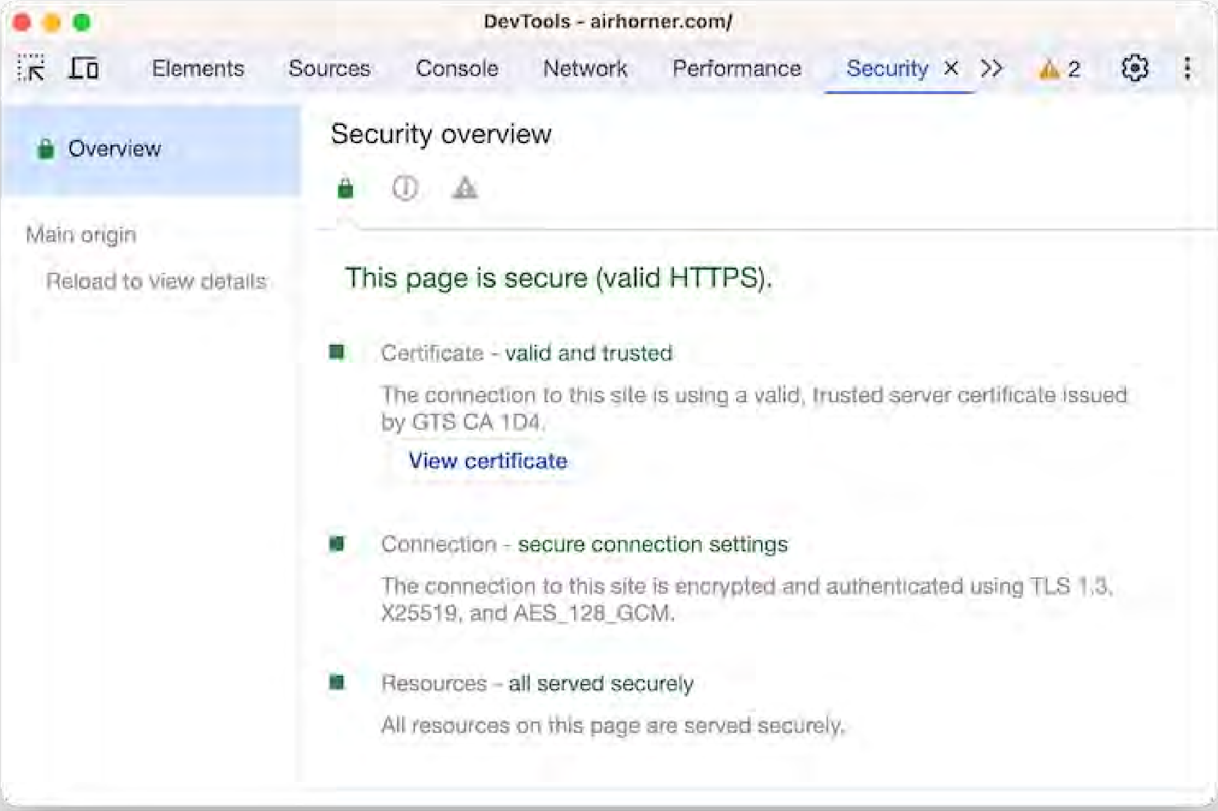
Update Cycle

Version	Update Activity	Timeline
#25	Install	
#25	Wait	
#25	Activate	

Inspect all resources that are loaded, including IndexedDB or Web SQL databases, local and session storage, cookies, Application Cache, images, fonts, and stylesheets.

- Debug Progressive Web Apps
- View and edit local storage
- View, add, edit, and delete cookies
- View origin trial information

Security panel



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by GTS CA 1D4.

View certificate

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

Debug mixed content issues, certificate problems, and more.

Understand security issues

Community

File bug reports and feature requests in Crbug, which is the engineering team's bug tracker.

Crbug

If you want to alert us to a bug or feature request but don't have much time, you're welcome to

For help with using DevTools, Stack Overflow is the best channel.

Stack Overflow

To file bugs or feature requests on the DevTools docs, open a GitHub issue.

Docs Issues

DevTools also has a Slack channel, but the team doesn't monitor it consistently.

Slack

Published on Monday, March 28, 2016 • Improve article

Follow us

Contribute

File a bug

View source

Related content

Connect

Twitter

YouTube

GitHub

Google for Developers

Chrome Firebase Generative AI All products Privacy Terms

ENGLISH (en)

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #449

Firefox accounts will be renamed Mozilla accounts on Nov 1

You'll still sign in with the same username and password, and there are no other changes to the products that you use. You may see updated help articles that refer to Mozilla accounts before Nov 1.

Learn more

Support
moz://a

Protect your privacy

Find help...

Customize this article

Download Firefox

Systems and Languages What's New Privacy

Common Myths about Private Browsing

Private Browsing is a useful feature of Firefox, but only if you understand the protection it offers. It helps you obscure your online activity from other people who use Firefox on your computer, but does not make you invisible online.

Myth 1: Private Browsing makes you anonymous on the Internet

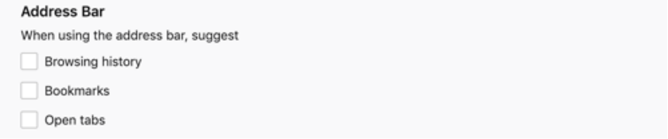
Reality: Private Browsing does not mask your identity or activity online. Websites and internet service providers can still gather information about your visit, even if you are not signed in. If you use your device at work, your company may be able to monitor the websites you visit. If you surf the Web at home, your cable company (or their partners) may have access to your browsing information. Only a Virtual Private Network (VPN) can mask your location and encrypt your online activity, keeping your identity and data safe from prying eyes. If you need to stay anonymous online, try Mozilla VPN.

Myth 2: Private Browsing removes all traces of your browsing activity from your computer

Reality: Private Browsing works by letting you browse without saving passwords, cookies and browsing history in a Private Window. If you download a file from a website, it will remain on your computer, but it will not appear in the download manager in Firefox. If you bookmark a website while in a Private Window, it will remain in your bookmark list.

Myth 3: Private Browsing doesn't display any browsing history

Reality: Private Browsing will, by default, display visited sites and bookmarks as you type in the address bar. Firefox saves these pages during normal browsing. If you don't want to see these suggestions, you can deselect them in your Firefox Settings Privacy & Security panel under *Address Bar*.



Address Bar

When using the address bar, suggest

□ Browsing history

□ Bookmarks

□ Open tabs

Myth 4: Private Browsing will protect you from keystroke loggers and spyware

Reality: Private Browsing does not protect you from malware installed on your computer. If you suspect you have malware, take steps to remove it to prevent it from happening again.

To learn more about how Firefox protects your privacy, see Enhanced Tracking Protection in Firefox for desktop and SmartBlock for Enhanced Tracking Protection.

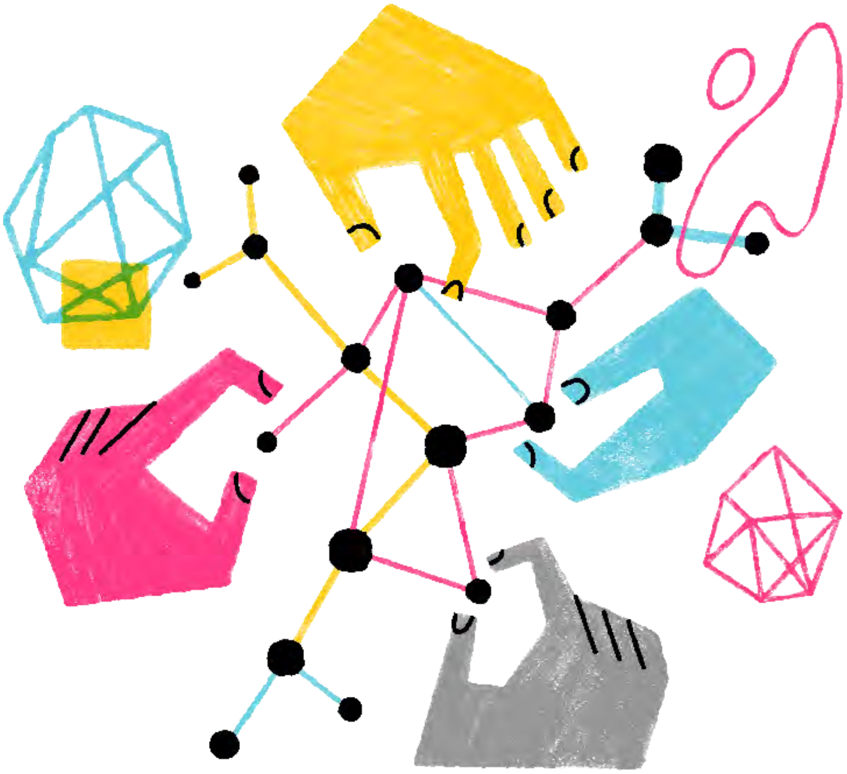
Share this article: https://mzl.la/3QEJeo1

Was this article helpful?

👍 👎

These fine people helped write this article:

AliceWyman, Michele Rodaro, Mozinet, Joni, Artist, Jeff, Erin S., Fabi, k_alex, Bithiah, JeremyKoozar, alineee



Volunteer

Grow and share your expertise with others. Answer questions and improve our knowledge base.

Learn More

Twitter

Join our Community

Explore Help Articles

Firefox Accounts

Sign In/Up

Benefits

Android Browser

iOS Browser

Focus Browser

Language

English

Beta for Android

Nightly

Nightly for Android

mozilla.org Terms of Service Privacy Cookies Contact

Visit Mozilla Corporation’s not-for-profit parent, the Mozilla Foundation.

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #476

moz://a

Incognito browser: What it really means

Firefox calls it private browsing, Chrome calls it incognito mode. Both let you browse the web without saving your browsing history.

Download Firefox

Firefox Privacy Notice

What Incognito/Private Mode Does

Incognito or private mode keeps your browsing history private. That’s it.

What Incognito/Private Mode Doesn’t Do

A 2018 survey of 460 internet users by the University of Chicago found that there are a lot of misconceptions out there about private browsing or incognito mode. It won't protect you from viruses or malware. It won't keep your internet service provider (ISP) from seeing where you've been online. It won't stop websites from seeing your physical location. And any bookmarks you save while in private browsing or incognito mode won't disappear when you switch it off.

Why go private/incognito?

Just because you're using private browsing mode doesn't mean you're up to something nefarious. Perhaps you want to keep your work and personal life separate. You might share a computer or device and you don't want your siblings snooping. You could be shopping for a gift and you don't want anything to spoil the surprise. Or maybe you just want to limit the amount of data companies collect about you and you value privacy. Incognito or private browsing mode is made for any of these scenarios.

Web Tracking

A lot of sites keep track of your browsing activity. Most do it to understand if you're interested in purchasing a product or clicking on an article. They can also do it to help make their sites easier to use. But almost all tracking is done to serve you ads.

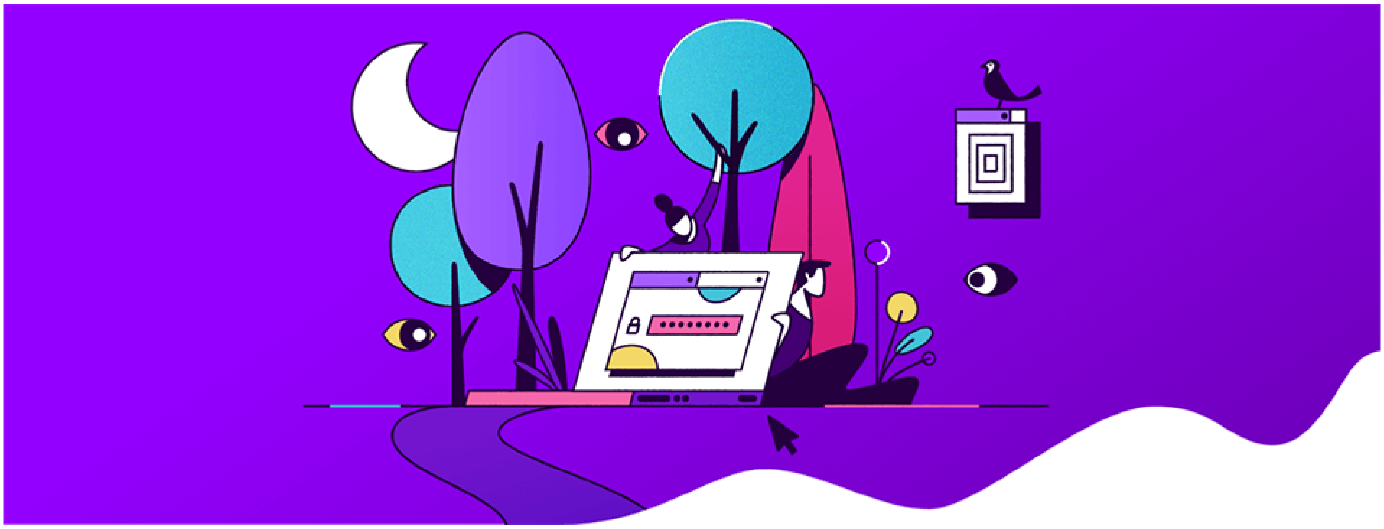
Online ads are customized based on your browsing. Been searching for a new pair of sandals? "Shoe Store X" has a great deal for you. The company knows where you've been because they dropped a bit of code into your browser called a cookie. The cookie tracks you, and so do Shoe Store X ads.

Cookies

Cookies were first used to customize websites, keep track of shopping carts, and maintain online account security, but today most are used to help companies serve targeted ads.

Here's how it works: You visit a site, an advertiser leaves a cookie on your browser. The cookie is your unique ID. Your information is stored in the cloud along with that ID. That can include which sites you visited, how long you visited them, what you clicked on, your language preferences and more.

Cookies also help advertisers deliver ads in your social media feeds. Social sites have their own tracking schemes and they're far more robust. They can track every click, post, and comment. In addition, cookies can report what you've been doing online to a social site, which is how some ads follow you into social media.



Going Incognito

So you've decided to keep to yourself online, to go incognito or enter private browsing mode. What does that mean? In Firefox, Private Browsing deletes cookie data when you close the browser window and doesn't track your browsing data. It also blocks tracking cookies by default. Finally, it won't remember any files you download, but those files will still be on your computer.

In Chrome, incognito mode does the same thing. In either case, your actions could be visible to the websites you visit, your employer or school, or your internet service provider (ISP). Also, if you sign into any accounts, your browsing activity may be saved to that account. And chances are if you're using Chrome, you'll be logged into your Google account.

Firefox Tracking Protection

Firefox goes beyond private browsing with Tracking Protection. It stops companies from following you around the web. It uses a list of tracking sites compiled by Disconnect.me. Whenever a cookie tries to reach a site on the list, Tracking Protection blocks it.

Firefox Multi-Account Containers

The Firefox Multi-Account Containers add-on isn't technically a form of private browsing or tracking protection, but it can help keep companies from knowing everything you do online. It lets you open fresh, cookie-free tabs that can be used for different accounts—personal, work, shopping, etc. That means you can use Multi-Account Containers to open several Google accounts at once without any overlap. Most trackers won't associate the different accounts, keeping your work life separate from your personal life online. Some more advanced trackers, however, can and will track you across different accounts, so beware.

Is Incognito/Private Mode Really Private?

Incognito or private mode will keep your local browsing private, but it won't stop your ISP, school, or employer from seeing where you've been online. In fact, your ISP has access to all your browsing activity pretty much no matter what you do.

You can, however, use a Virtual Private Network (VPN) service. VPN services route traffic through remote servers, so it looks like you're browsing from another location or multiple locations. VPN providers can track where you've been online, though, so it's good to find a company you can trust to either delete or lock up your browsing activity. VPNs won't block third-party cookies from advertisers, but those cookies won't be able to identify your location accurately, making it difficult or impossible for ad trackers to be effective.

Tor Browser can truly mask your online activity. It bounces traffic through multiple servers around the globe, making it difficult to track that traffic. The website you visit really has no idea where you are, only the approximate location of the last server your request was routed through. But again, even Tor proxy won't stop third-party advertisers from installing cookies in your browser. Tor Browser deletes all cookies when closed. People can also start a new session in Tor Browser to clear them as well.

Incognito: TL:DR

Incognito mode keeps your browser history private, and that's pretty much it. If you want more privacy, you'll need to add Tracking Protection and maybe even browse through a Virtual Private Network (VPN) service. Incognito mode can't.

Take control of your browser.

Download Firefox

Firefox Privacy Notice

Company

Mozilla Manifesto

Press Center

Corporate Blog

Careers

Contact

Donate

Resources

Privacy Hub

Browser Comparison

Brand Standards

Support

Product Help

File a Bug

Localize Mozilla

Developers

Developer Edition

Beta

Beta for Android

Nightly

Nightly for Android

Enterprise

Tools

Follow @Mozilla

Follow @Firefox

Website Privacy Notice Cookies Legal Community Participation Guidelines About this site

Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #486

Support
moz://a

Protect your privacy

Find help...

Customize this article

Download Firefox

Systems and Languages What's New Privacy

Private Browsing - Use Firefox without saving history

Private Browsing does not save your browsing information, such as history and cookies, and leaves no trace after you end the session. By default, when you browse in private windows, you're shielded from third-party cookies and content trackers. Our Anti-Tracking Policy reflects our commitment to protecting your privacy and keeping you secure. Firefox also has Enhanced Tracking Protection, which prevents hidden trackers from collecting your data across multiple sites and slowing down your browsing.

Want to learn more? See the SmartBlock for Enhanced Tracking Protection article.

Important: Private Browsing does not make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still gather information about pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer. To learn more, see Common Myths about Private Browsing.

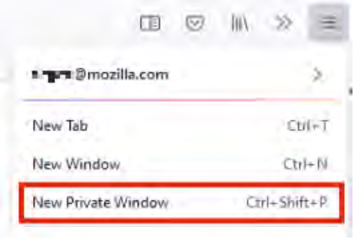
Table of Contents

How do I open a new Private Window?

There are two ways to open a new Private Window:

Open a new Private Window from the Firefox menu

- Click the menu button ☰ and then click New Private Window .



The Private Browsing home page will open in a new window.

Open a link in a new Private Window

- Right-click on any link and choose Open Link in New Private Window from the context menu.

Tip: Private Browsing windows have a purple mask at the top.

What does Private Browsing not save?

- **Visited pages:** Pages will not be added to the list of sites in the History menu, the Library window's history list, nor in the address bar drop-down list.
- **Form and Search Bar entries:** Nothing you enter into text boxes on web pages nor the Search bar will be saved for Form autocomplete.
- **Download List entries:** Files you download will not be listed in the Downloads Library after you turn off Private Browsing.
- **Cookies:** Cookies store information about websites you visit, such as site preferences, and login status. Cookies can also be used by third parties to track you across websites. See the How do I turn on the Do Not Track feature? article to learn more about tracking. Cookies set in private windows are held temporarily in memory, separate from regular window cookies, and discarded at the end of your private session (after the last private window is closed).
- **Cached Web Content** and **Offline Web Content and User Data:** Temporary Internet files (cached files) and files that websites save for offline use will not be saved.

Note:

- New passwords and bookmarks you create while using Private Browsing will be saved.
- Any files you download to your computer while using Private Browsing will be saved.

Can I set Firefox to always use Private Browsing?

Firefox is set to remember history by default, but you can change this setting in your Firefox Privacy Settings :

1. Click the menu button and select Settings .
2. Select the Privacy & Security panel and go to the **History** section.
3. Choose **Use custom settings for history** from the drop-down menu and check the **Always use private browsing mode** setting.
   - Alternatively, you can select **Never remember history** from the drop-down menu, which is equivalent to always being in Private Browsing mode.
4. Restart Firefox.

> **Important:** When Firefox is set to **Always use private browsing mode** or to **Never remember history**, you won't see a purple mask at the top of each window, even though you are in Private Browsing mode. To restore normal browsing, go to your Privacy & Security Settings and uncheck **Always use private browsing mode** from your **Use custom settings for history** settings (or select **Remember history** from the drop-down menu) and restart Firefox.

You can also **pin Firefox in Private Browsing mode to the Windows taskbar** for easy access:

1. Click the Menu button and select New Private Window . A new Firefox icon with a small purple mask will show in the Windows taskbar, this is the Private Browsing mode icon.
2. Right-click the Firefox in Private Browsing mode icon in the taskbar.
3. Click **Pin to taskbar**.

Other ways to control what information Firefox saves

- You can always remove recent browsing, search and download history after visiting a site.
- Read more articles on this topic: Passwords, forms, search, and history - control what Firefox suggests.

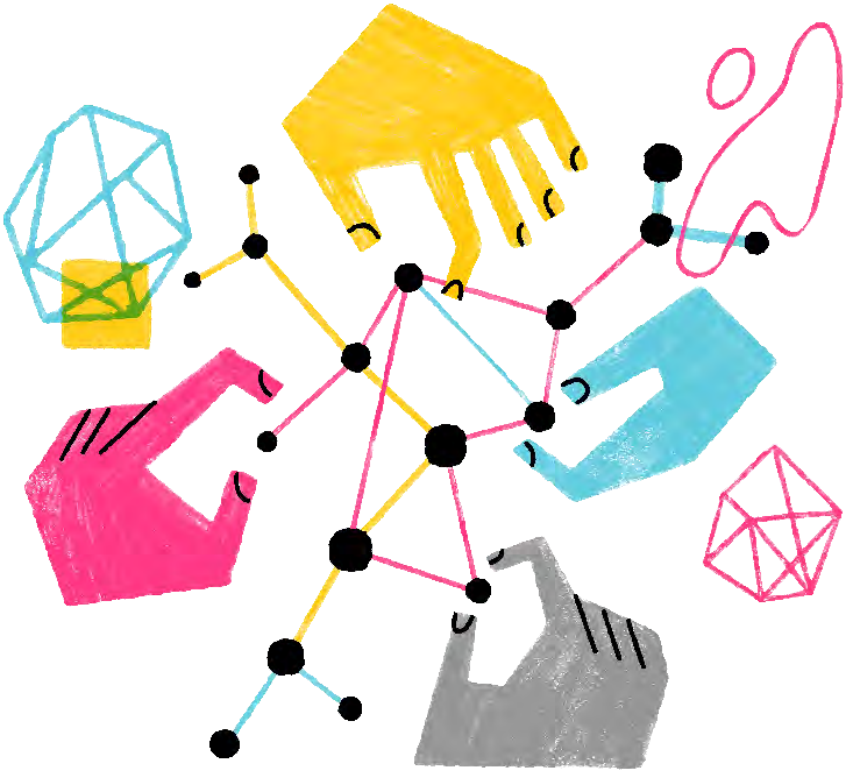
Share this article: http://mzl.la/1NATRAg

Was this article helpful?

👍 👎

These fine people helped write this article:

AliceWyman, jscher2000 - Support Volunteer, Cheng Wang, Underpass, novica, Tonnes, Michele Rodaro, Jan., Michael Verdi, scoobidiver, TyDraniu, Swarnava Sengupta, Ben, Centinel, Mozinet, user669794, adampeebleswrites, Wesley Branton, Lan, user955666, Joni, Artist, vesper, tech53, Angela Lazar, ErlingR, PGGWriter, biddutbbb.2224, Fabi, k_alex



Volunteer

Grow and share your expertise with others. Answer questions and improve our knowledge base.

Learn More

Mozilla

Report Trademark Abuse

Source code

Twitter

Join our Community

Explore Help Articles

Firefox Accounts

Sign In/Up

Benefits

Firefox

Download

Firefox Desktop

Android Browser

iOS Browser

Focus Browser

Language

English

Firefox for Developers

Developer Edition

Beta

Beta for Android

Nightly

Nightly for Android

Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.

mozilla.org Terms of Service Privacy Cookies Contact

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #487

Inspect network activity

Published on Friday, February 8, 2019

Get started Find issues

Kayce Basques
Technically, I'm a writer
Twitter GitHub Glitch

Table of contents ▾

This is a hands-on tutorial of some of the most commonly-used DevTools features related to inspecting a page's network activity.

See Network Reference if you'd like to browse features instead.

Read on, or watch the video version of this tutorial:

When to use the Network panel

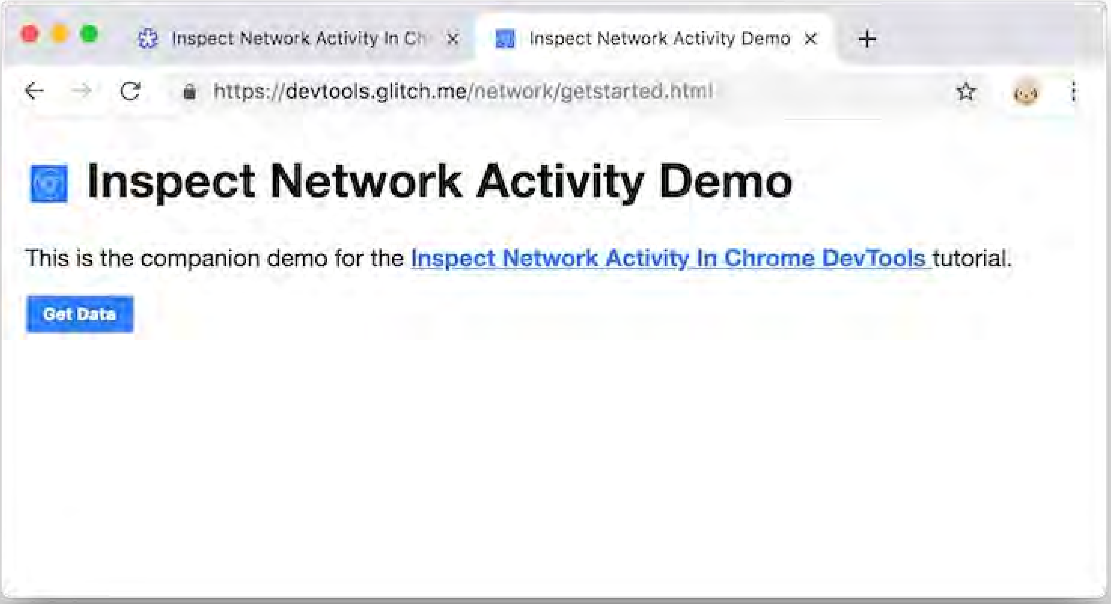
In general, use the Network panel when you need to make sure that resources are being downloaded or uploaded as expected. The most common use cases for the Network panel are:

Making sure that resources are actually being uploaded or downloaded at all.

Inspecting the properties of an individual resource, such as its HTTP headers, content, size, and so on.

If you're looking for ways to improve page load performance, *don't* start with the Network panel. There are many types of load performance issues that aren't related to network activity. Start with the Audits panel because it gives you targeted suggestions on how to improve your page. See Optimize Website Speed.

1 Open the Get Started Demo.

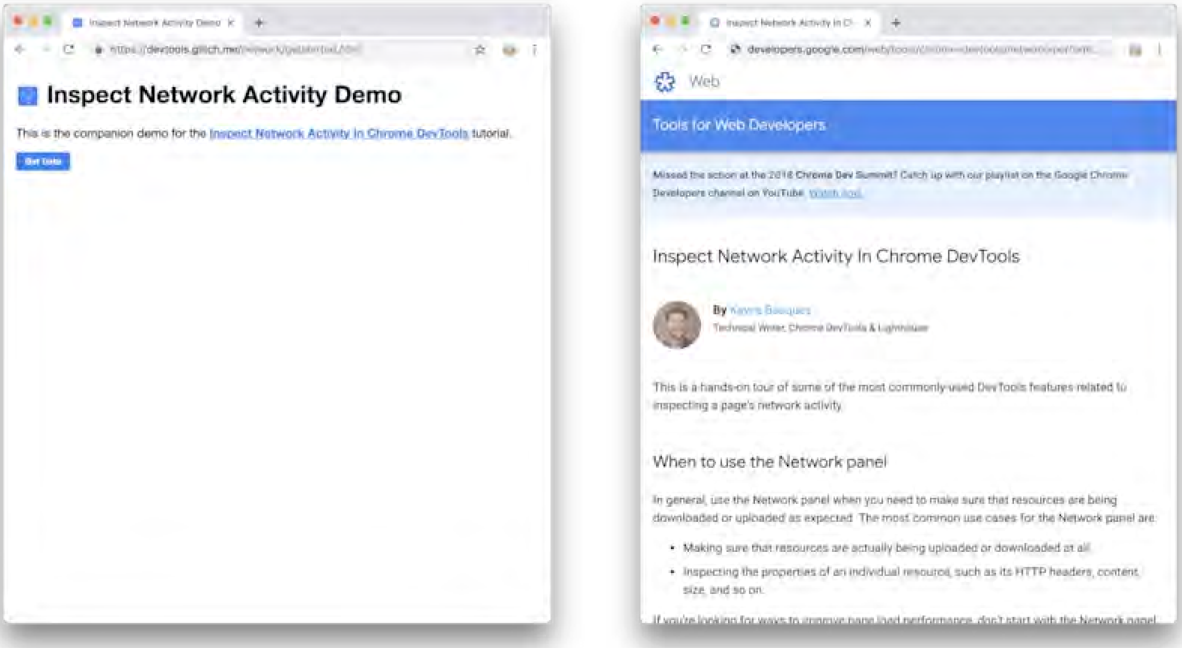

Inspect Network Activity In Ch
Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Figure 1. The demo

You might prefer to move the demo to a separate window.


Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data
Inspect Network Activity In Ch
developers.google.com/web/tools/chrome-devtools/network/perform...
Web
Tools for Web Developers

Missed the action at the 2018 Chrome Dev Summit? Catch up with our playlist on the Google Chrome Developers channel on YouTube. Watch now.

Inspect Network Activity In Chrome DevTools

By Kayce Basques
Technical Writer, Chrome DevTools & Lighthouse

This is a hands-on tour of some of the most commonly-used DevTools features related to inspecting a page's network activity.

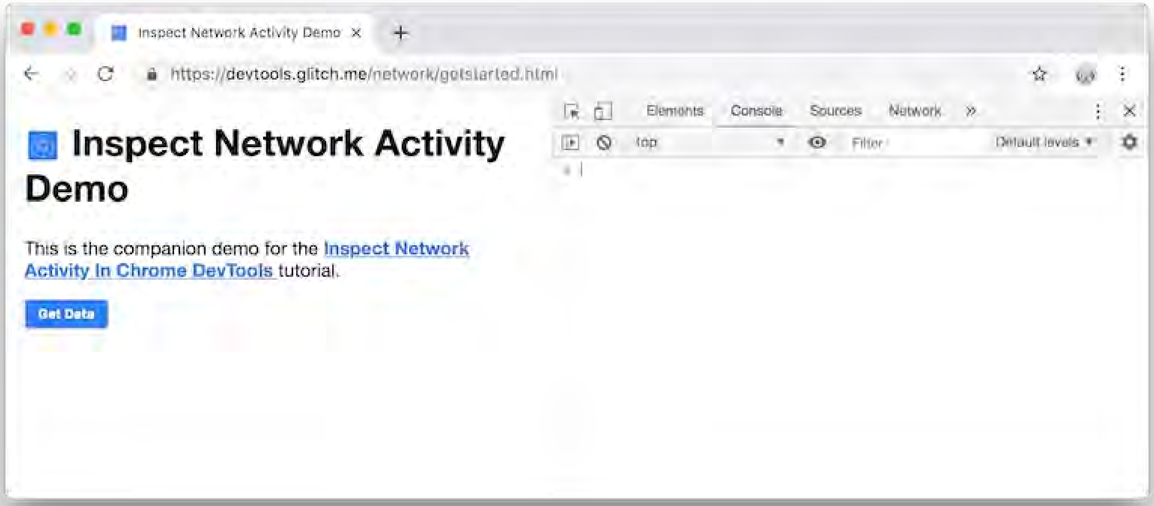
When to use the Network panel

In general, use the Network panel when you need to make sure that resources are being downloaded or uploaded as expected. The most common use cases for the Network panel are:

- Making sure that resources are actually being uploaded or downloaded at all.
- Inspecting the properties of an individual resource, such as its HTTP headers, content, size, and so on.

If you're looking for ways to improve page load performance, don't start with the Network panel

Figure 2. The demo in one window and this tutorial in a different window

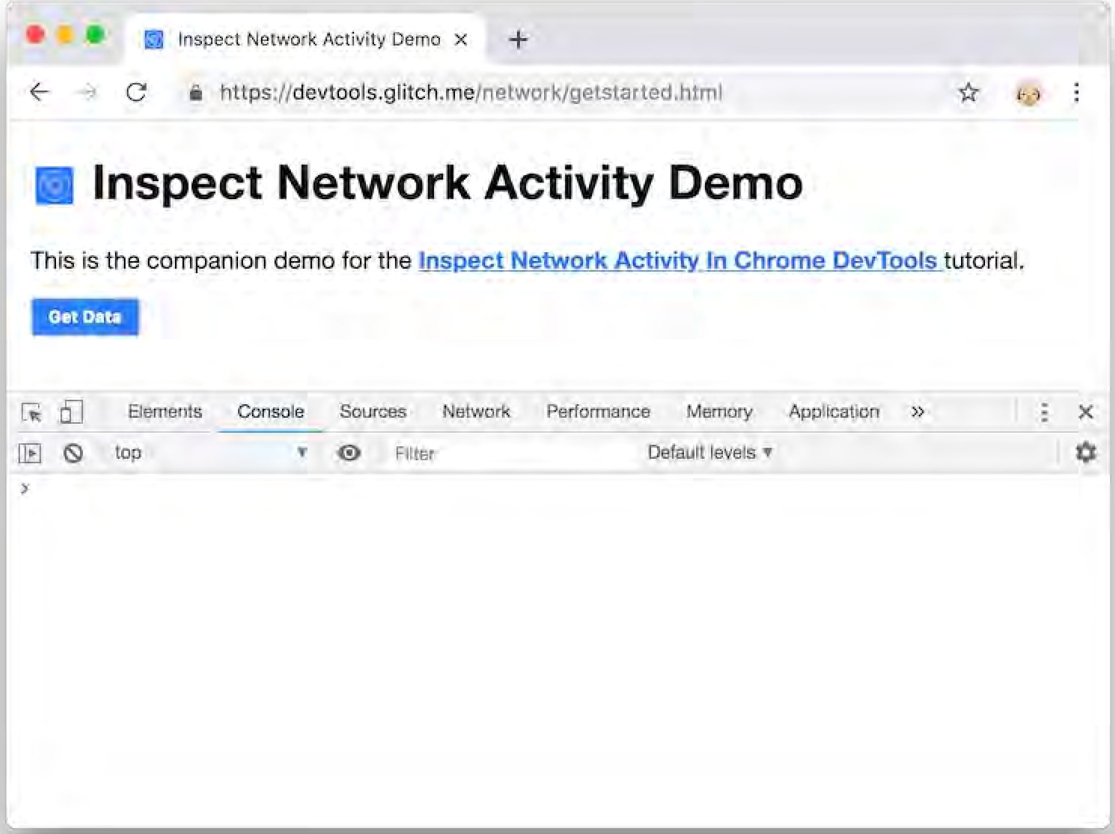

Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Elements
Console
Sources
Network
top
Filter
Default levels
Get Data

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Figure 3. The Console

You might prefer to dock DevTools to the bottom of your window.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

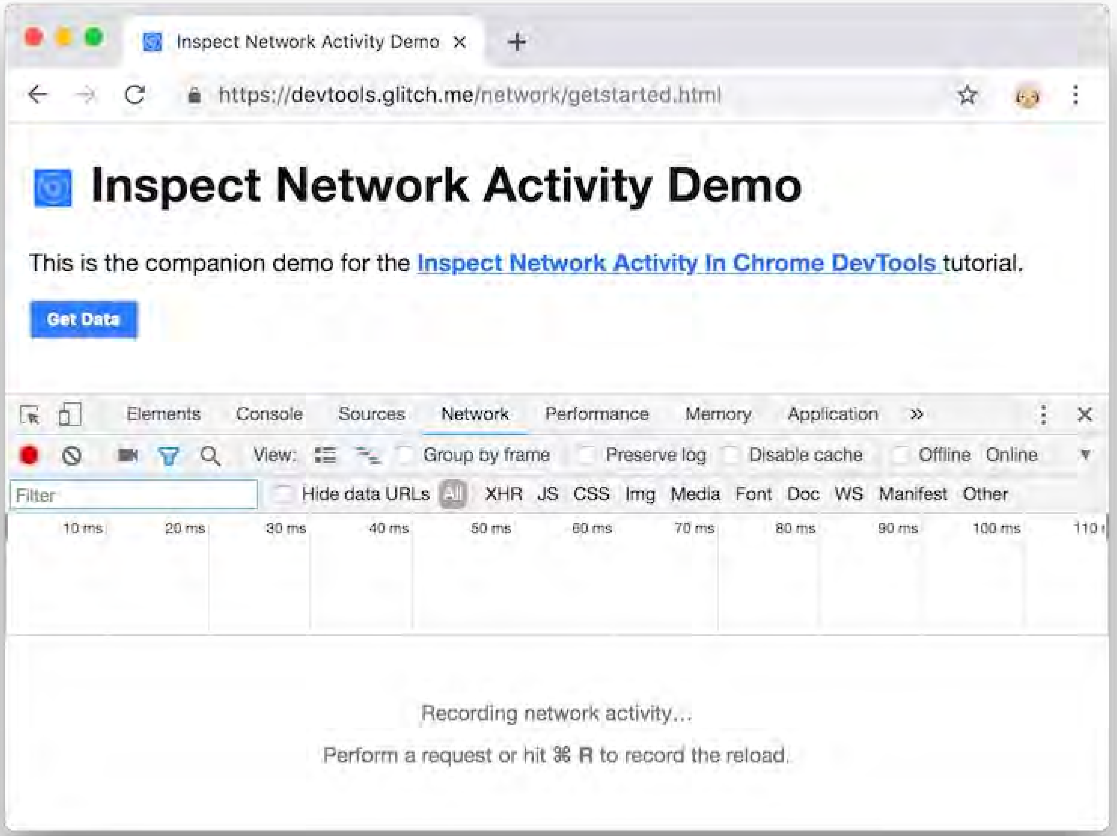

Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html
Inspect Network Activity Demo
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.
Get Data
Elements
Console
Sources
Network
Performance
Memory
Application
View:
Group by frame
Preserve log
Disable cache
Offline
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
10 ms
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
80 ms
90 ms
100 ms
110
Recording network activity...
Perform a request or hit ⌘ R to record the reload.

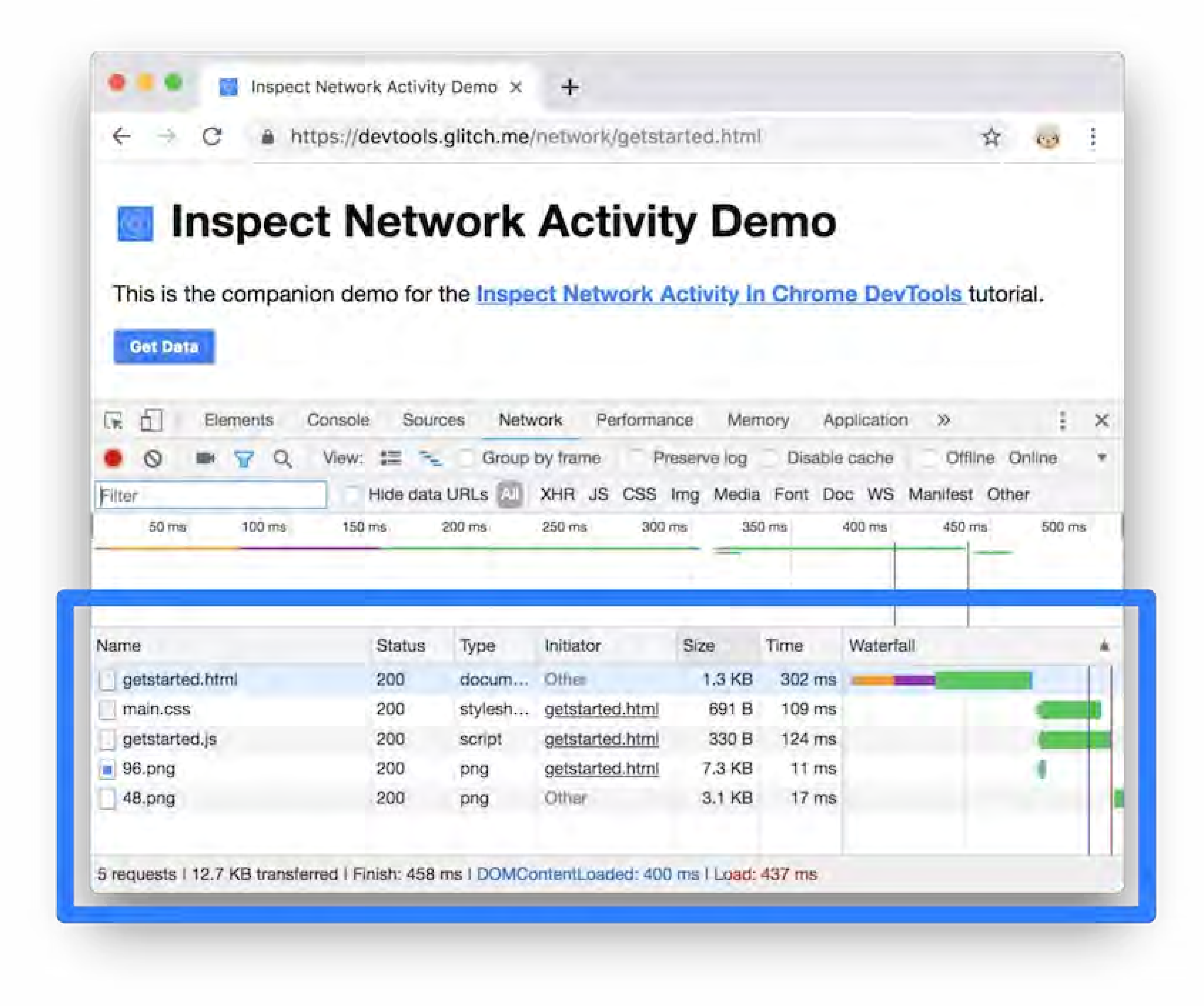
Figure 5. DevTools docked to the bottom of the window

Right now the Network panel is empty. That's because DevTools only logs network activity while it's open and no network activity has occurred since you opened DevTools.

Log network activity

To view the network activity that a page causes:

1 Reload the page. The Network panel logs all network activity in the **Network Log**.


Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Elements Console Sources Network Performance Memory Application »
View: Group by frame Preserve log Disable cache Offline Online
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
50 ms 100 ms 150 ms 200 ms 250 ms 300 ms 350 ms 400 ms 450 ms 500 ms

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum...	Other	1.3 KB	302 ms	
main.css	200	stylesh...	getstarted.html	691 B	109 ms	
getstarted.js	200	script	getstarted.html	330 B	124 ms	
96.png	200	png	getstarted.html	7.3 KB	11 ms	
48.png	200	png	Other	3.1 KB	17 ms	

5 requests | 12.7 KB transferred | Finish: 458 ms | DOMContentLoaded: 400 ms | Load: 437 ms

Figure 6. The Network Log

Each row of the **Network Log** represents a resource. By default the resources are listed chronologically. The top resource is usually the main HTML document. The bottom resource is whatever was requested last.

Each column represents information about a resource. **Figure 6** shows the default columns:

Status. The HTTP response code.

Type. The resource type.

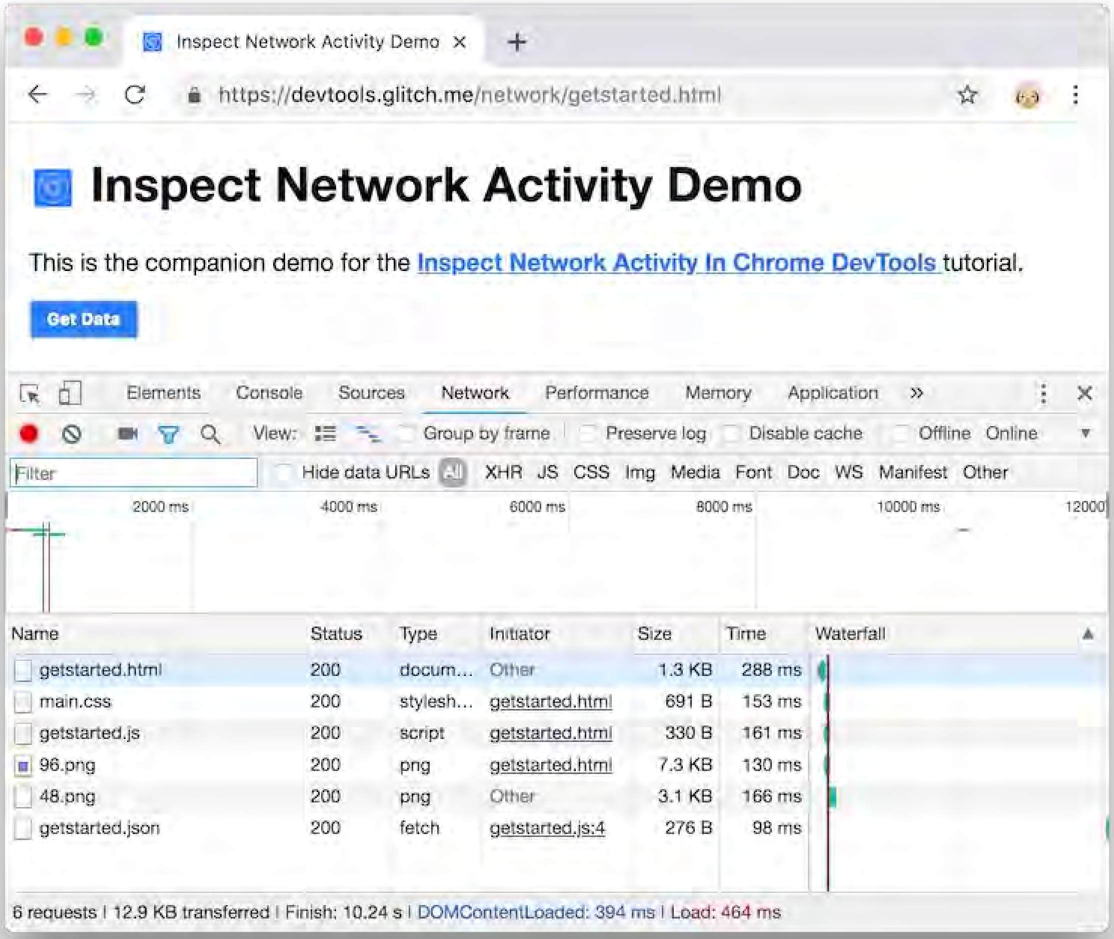
Initiator. What caused a resource to be requested. Clicking a link in the Initiator column takes you to the source code that caused the request.

Note The graph above the Network Log is called the Overview. You won't be using it in this tutorial, so you can hide it if you prefer. See Hide the Overview pane.

2 So long as you've got DevTools open, it will record network activity in the Network Log. To demonstrate this, first look at the bottom of the **Network Log** and make a mental note of the last activity.

3 Now, click the **Get Data** button in the demo.

4 Look at the bottom of the **Network Log** again. There's a new resource called `getstarted.json`. Clicking the **Get Data** button caused the page to request this file.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

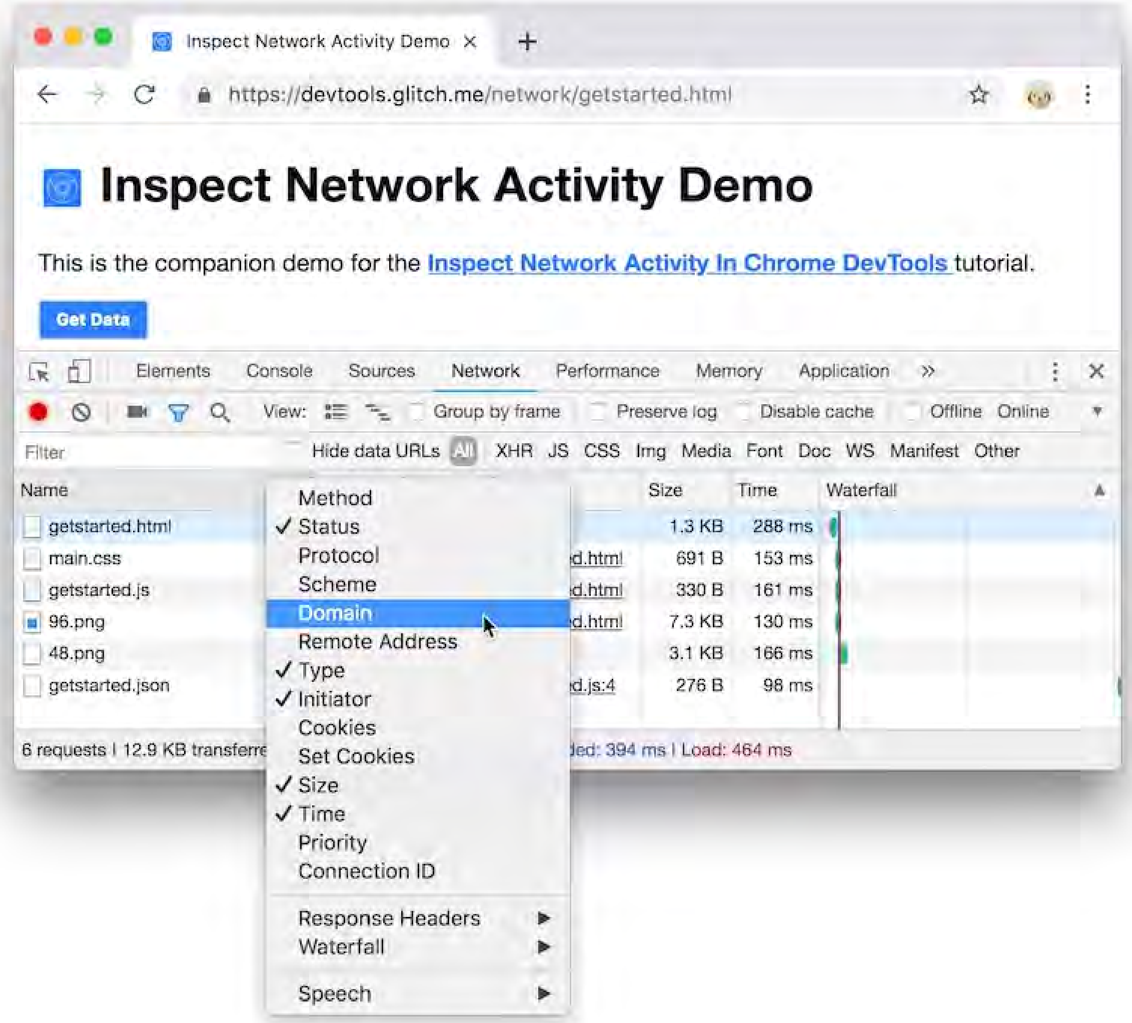
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum…	Other	1.3 KB	288 ms	
main.css	200	stylesh…	getstarted.html	691 B	153 ms	
getstarted.js	200	script	getstarted.html	330 B	161 ms	
96.png	200	png	getstarted.html	7.3 KB	130 ms	
48.png	200	png	Other	3.1 KB	166 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	98 ms	

6 requests | 12.9 KB transferred | Finish: 10.24 s | DOMContentLoaded: 394 ms | Load: 464 ms

The columns of the Network Log are configurable. You can hide columns that you're not using. There are also many columns that are hidden by default which you may find useful.

1 Right-click the header of the Network Log table and select **Domain**. The domain of each resource is now shown.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

Name		Size	Time	Waterfall
getstarted.html		1.3 KB	288 ms	
main.css	d.html	691 B	153 ms	
getstarted.js	d.html	330 B	161 ms	
96.png	d.html	7.3 KB	130 ms	
48.png		3.1 KB	166 ms	
getstarted.json	d.js:4	276 B	98 ms	

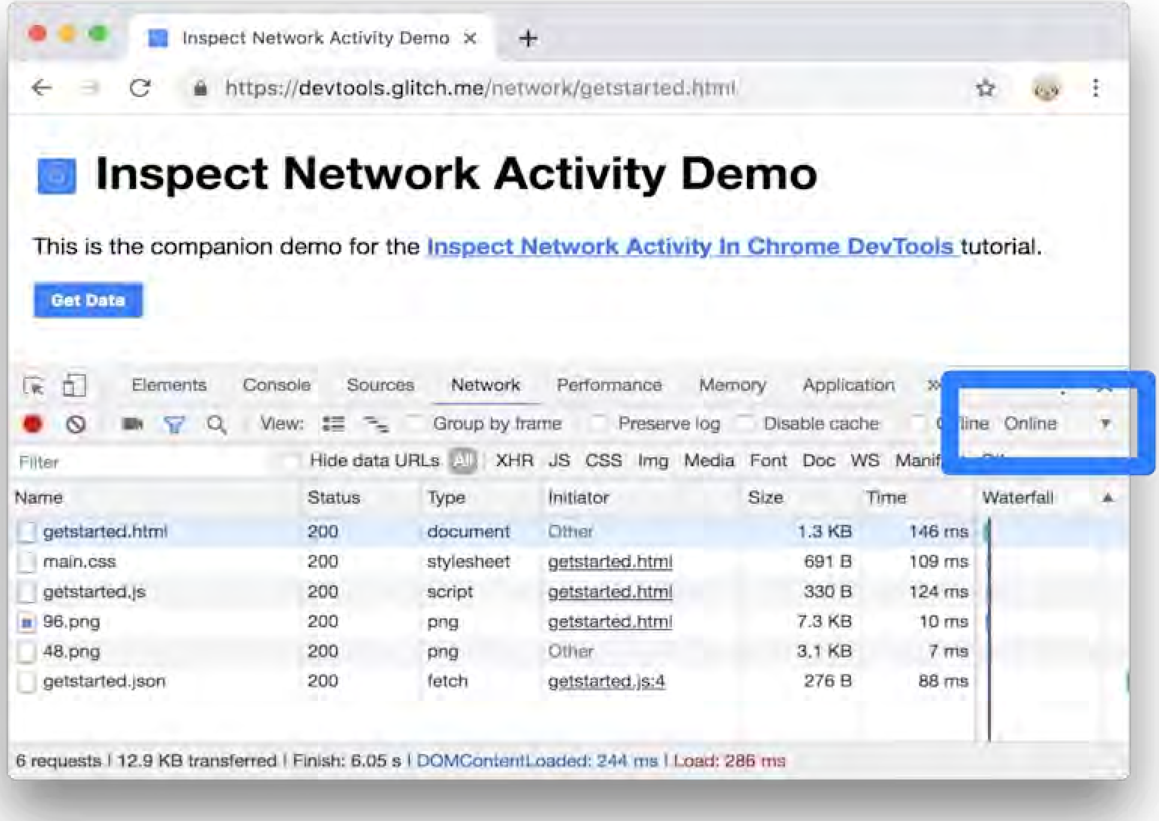
6 requests | 12.9 KB transferre ... led: 394 ms | Load: 464 ms

Figure 8. Enabling the Domain column

Tip You can see the full URL of a resource by hovering over its cell in the **Name** column.

The network connection of the computer that you use to build sites is probably faster than the network connections of the mobile devices of your users. By throttling the page you can get a better idea of how long a page takes to load on a mobile device.

1 Click the **Throttling** dropdown, which is set to **Online** by default.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

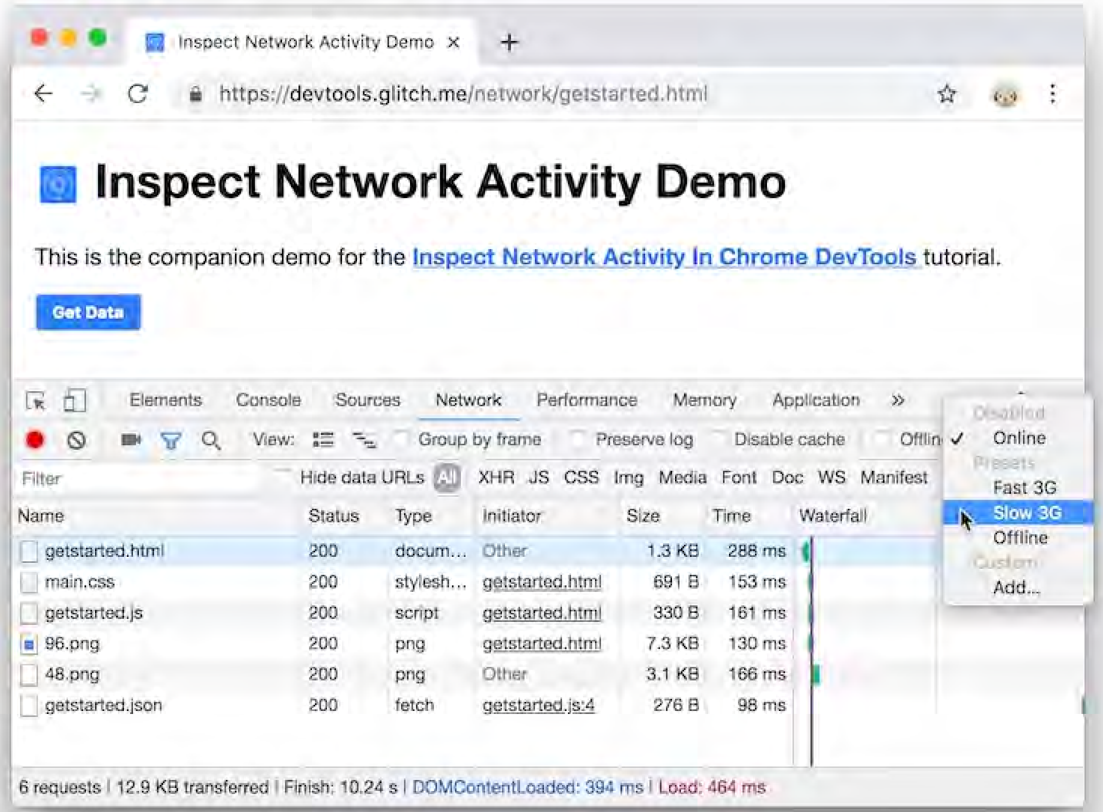
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	146 ms	
main.css	200	stylesheet	getstarted.html	691 B	109 ms	
getstarted.js	200	script	getstarted.html	330 B	124 ms	
96.png	200	png	getstarted.html	7.3 KB	10 ms	
48.png	200	png	Other	3.1 KB	7 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	88 ms	

6 requests | 12.9 KB transferred | Finish: 6.05 s | DOMContentLoaded: 244 ms | Load: 286 ms

Figure 9. Enabling throttling

2 Select **Slow 3G**.



https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

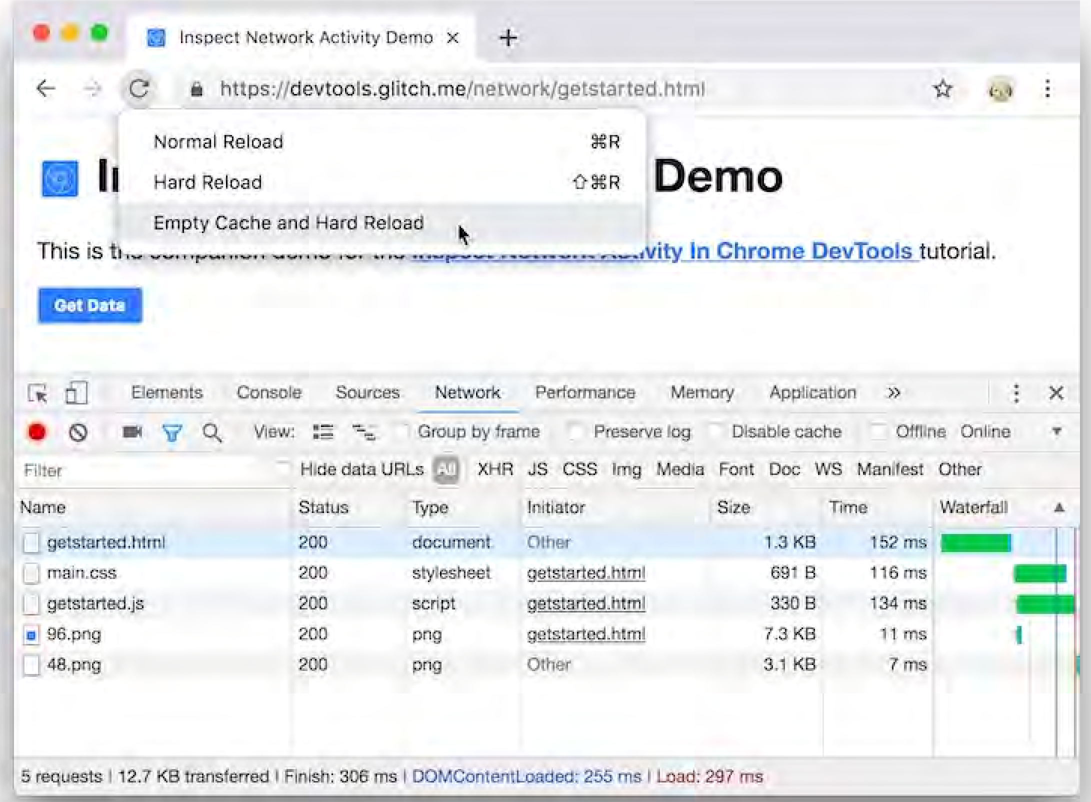
Get Data

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docum...	Other	1.3 KB	288 ms	
main.css	200	stylesh...	getstarted.html	691 B	153 ms	
getstarted.js	200	script	getstarted.html	330 B	161 ms	
96.png	200	png	getstarted.html	7.3 KB	130 ms	
48.png	200	png	Other	3.1 KB	166 ms	
getstarted.json	200	fetch	getstarted.js:4	276 B	98 ms	

6 requests | 12.9 KB transferred | Finish: 10.24 s | DOMContentLoaded: 394 ms | Load: 464 ms

Figure 10. Selecting Slow 3G

3 Long-press **Reload** ↻ and then select **Empty Cache And Hard Reload**.



Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	152 ms	
main.css	200	stylesheet	getstarted.html	691 B	116 ms	
getstarted.js	200	script	getstarted.html	330 B	134 ms	
96.png	200	png	getstarted.html	7.3 KB	11 ms	
48.png	200	png	Other	3.1 KB	7 ms	

5 requests | 12.7 KB transferred | Finish: 306 ms | DOMContentLoaded: 255 ms | Load: 297 ms

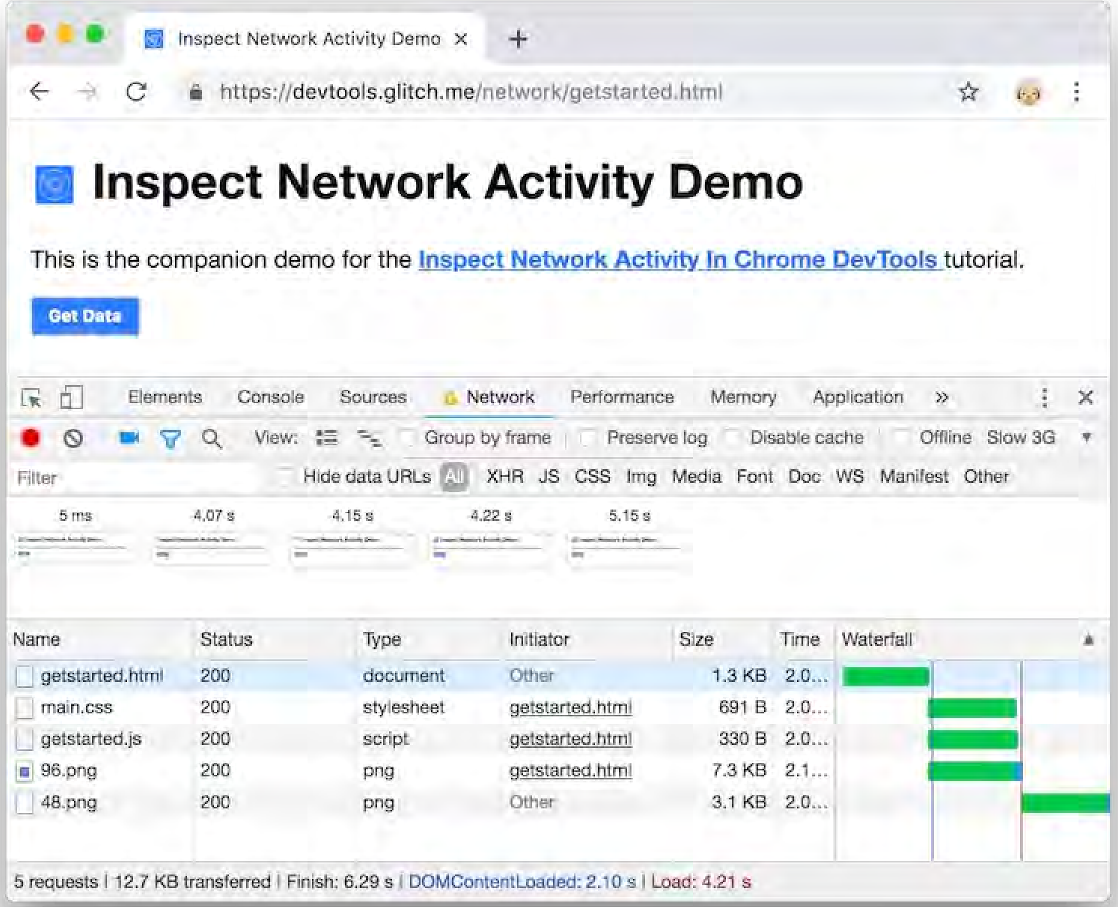
Figure 11. Empty Cache And Hard Reload

On repeat visits, the browser usually serves some files from its cache, which speeds up the page load. **Empty Cache And Hard Reload** forces the browser to go the network for all resources. This is helpful when you want to see how a first-time visitor experiences a page load.

> **Note** The **Empty Cache And Hard Reload** workflow is only available when DevTools is open.

Capture screenshots

2 Reload the page again via the **Empty Cache And Hard Reload** workflow. See Simulate a slower connection if you need a reminder on how to do this. The Screenshots pane provides thumbnails of how the page looked at various points during the loading process.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

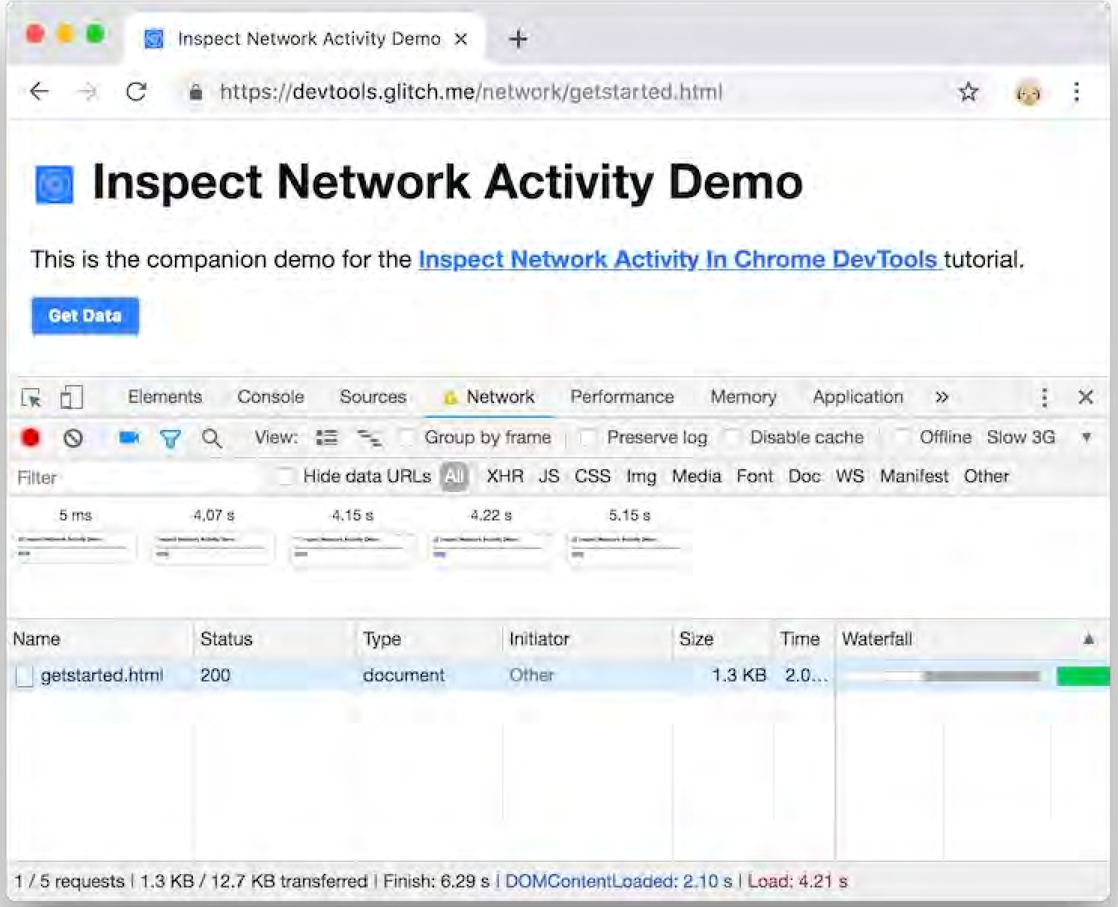
Slow 3G

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	2.0…	
main.css	200	stylesheet	getstarted.html	691 B	2.0…	
getstarted.js	200	script	getstarted.html	330 B	2.0…	
96.png	200	png	getstarted.html	7.3 KB	2.1…	
48.png	200	png	Other	3.1 KB	2.0…	

5 requests | 12.7 KB transferred | Finish: 6.29 s | DOMContentLoaded: 2.10 s | Load: 4.21 s

Figure 12. Screenshots of the page load

3 Click the first thumbnail. DevTools shows you what network activity was occurring at that moment in time.



Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	Other	1.3 KB	2.0...	

1 / 5 requests | 1.3 KB / 12.7 KB transferred | Finish: 6.29 s | DOMContentLoaded: 2.10 s | Load: 4.21 s

Figure 13. The network activity that was happening during the first screenshot

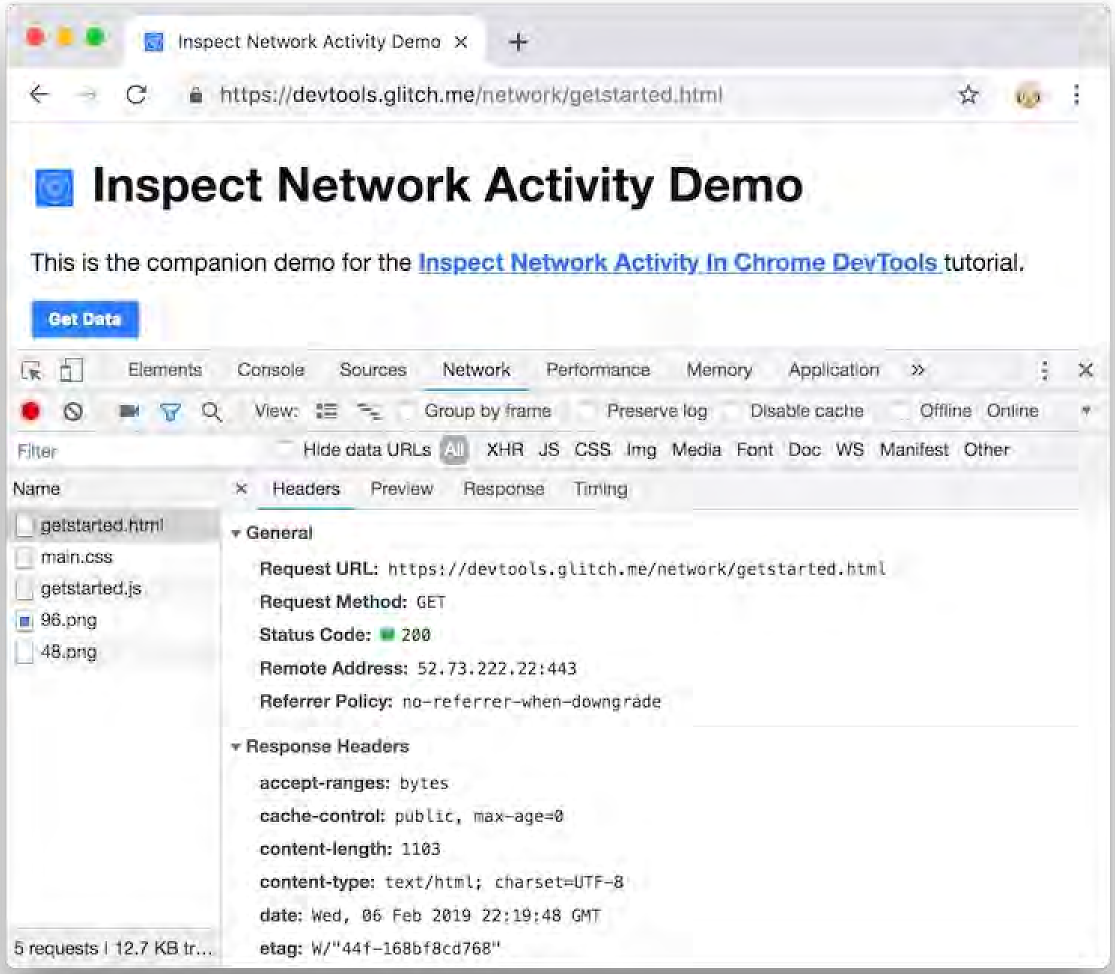
4 Click **Capture Screenshots** again to close the Screenshots pane.

5 Reload the page again.

Inspect a resource's details

Click a resource to learn more information about it. Try it now:

1 Click `getstarted.html`. The **Headers** tab is shown. Use this tab to inspect HTTP headers.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

▾ General

```
Request URL: https://devtools.glitch.me/network/getstarted.html
Request Method: GET
Status Code: 🟩 200
Remote Address: 52.73.222.22:443
Referrer Policy: no-referrer-when-downgrade
```

▾ Response Headers

```
accept-ranges: bytes
cache-control: public, max-age=0
content-length: 1103
content-type: text/html; charset=UTF-8
date: Wed, 06 Feb 2019 22:19:48 GMT
etag: W/"44f-168bf8cd768"
```

Figure 14. The Headers tab

2 Click the **Preview** tab. A basic rendering of the HTML is shown.

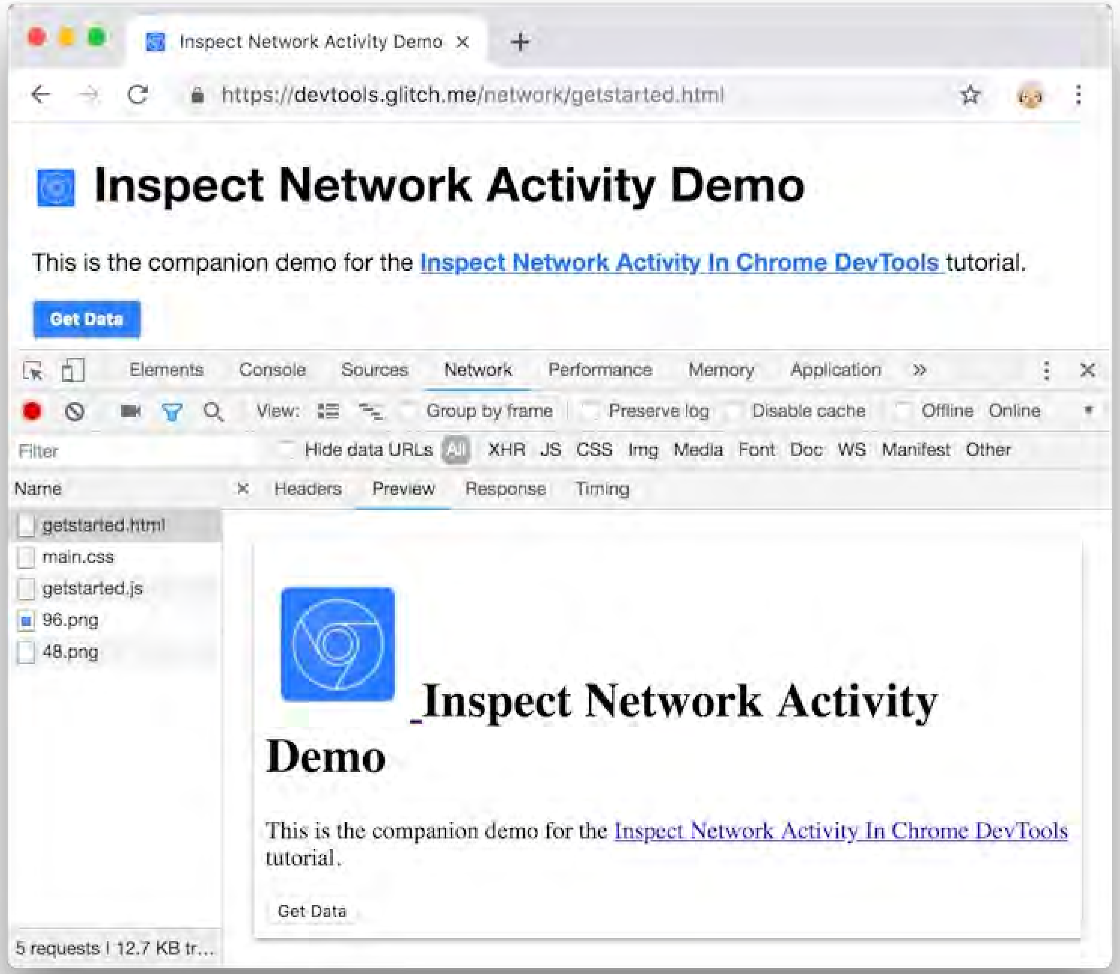
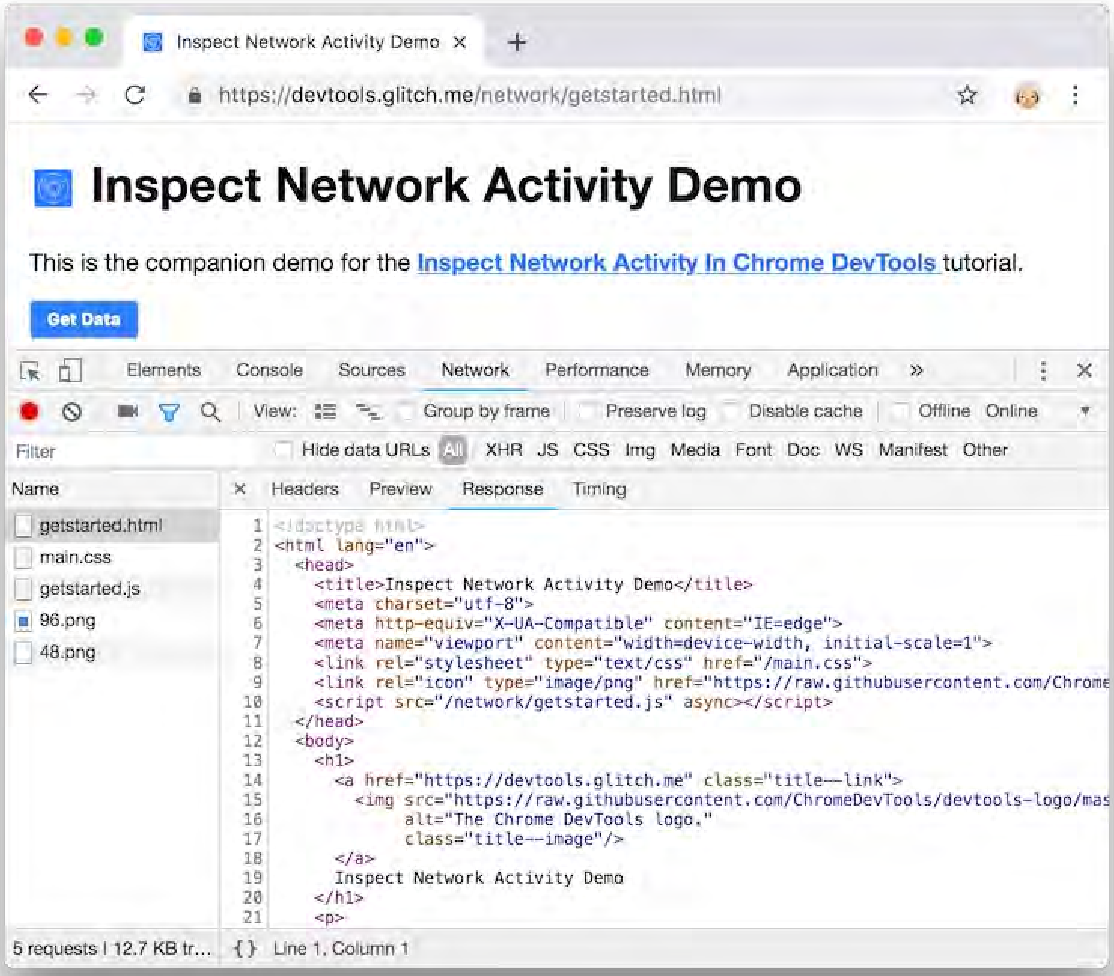

Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Inspect Network Activity Demo
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.
Get Data
Elements
Console
Sources
Network
Performance
Memory
Application
View:
Group by frame
Preserve log
Disable cache
Offline
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Name
Headers
Preview
Response
Timing
getstarted.html
main.css
getstarted.js
96.png
48.png
Inspect Network Activity Demo
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.
Get Data
5 requests | 12.7 KB tr...

Figure 15. The Preview tab

This tab is helpful when an API returns an error code in HTML and it's easier to read the rendered HTML than the HTML source code, or when inspecting images.

3 Click the **Response** tab. The HTML source code is shown.


Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html
Elements Console Sources Network Performance Memory Application »
View: Group by frame Preserve log Disable cache Offline Online
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
Name
getstarted.html
main.css
getstarted.js
96.png
48.png
× Headers Preview Response Timing
5 requests | 12.7 KB tr...
{ } Line 1, Column 1

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

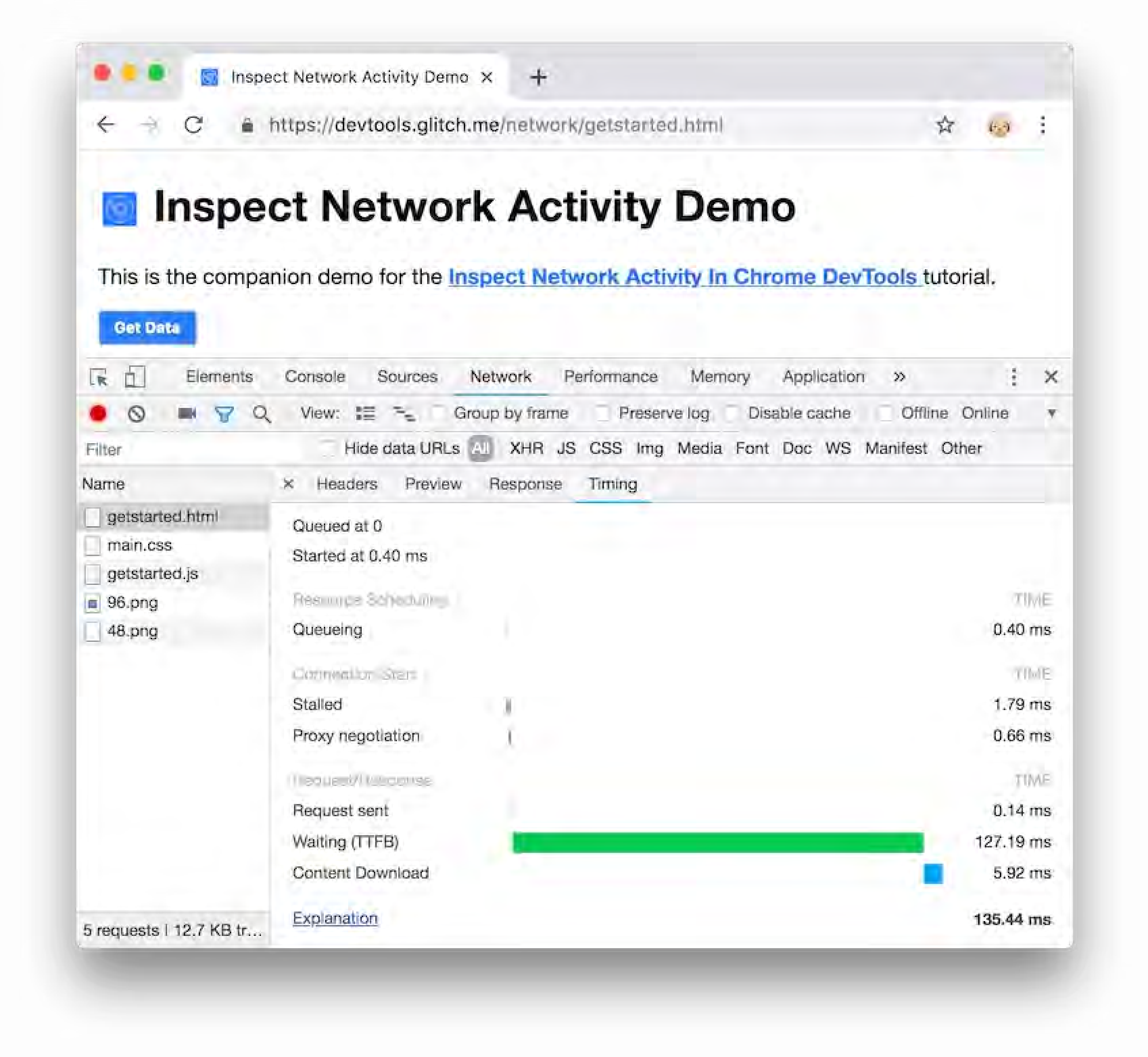
Get Data

```
<!doctype html>
<html lang="en">
  <head>
    <title>Inspect Network Activity Demo</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" href="/main.css">
    <link rel="icon" type="image/png" href="https://raw.githubusercontent.com/Chrome
    <script src="/network/getstarted.js" async></script>
  </head>
  <body>
    <h1>
      <a href="https://devtools.glitch.me" class="title--link">
        <img src="https://raw.githubusercontent.com/ChromeDevTools/devtools-logo/mas
             alt="The Chrome DevTools logo."
             class="title--image"/>
      </a>
      Inspect Network Activity Demo
    </h1>
    <p>
```

Figure 16. The Response tab

> **Tip** When a file is minified, clicking the **Format** { } button at the bottom of the **Response** tab re-formats the file's contents for readability.

4 Click the **Timing** tab. A breakdown of the network activity for this resource is shown.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

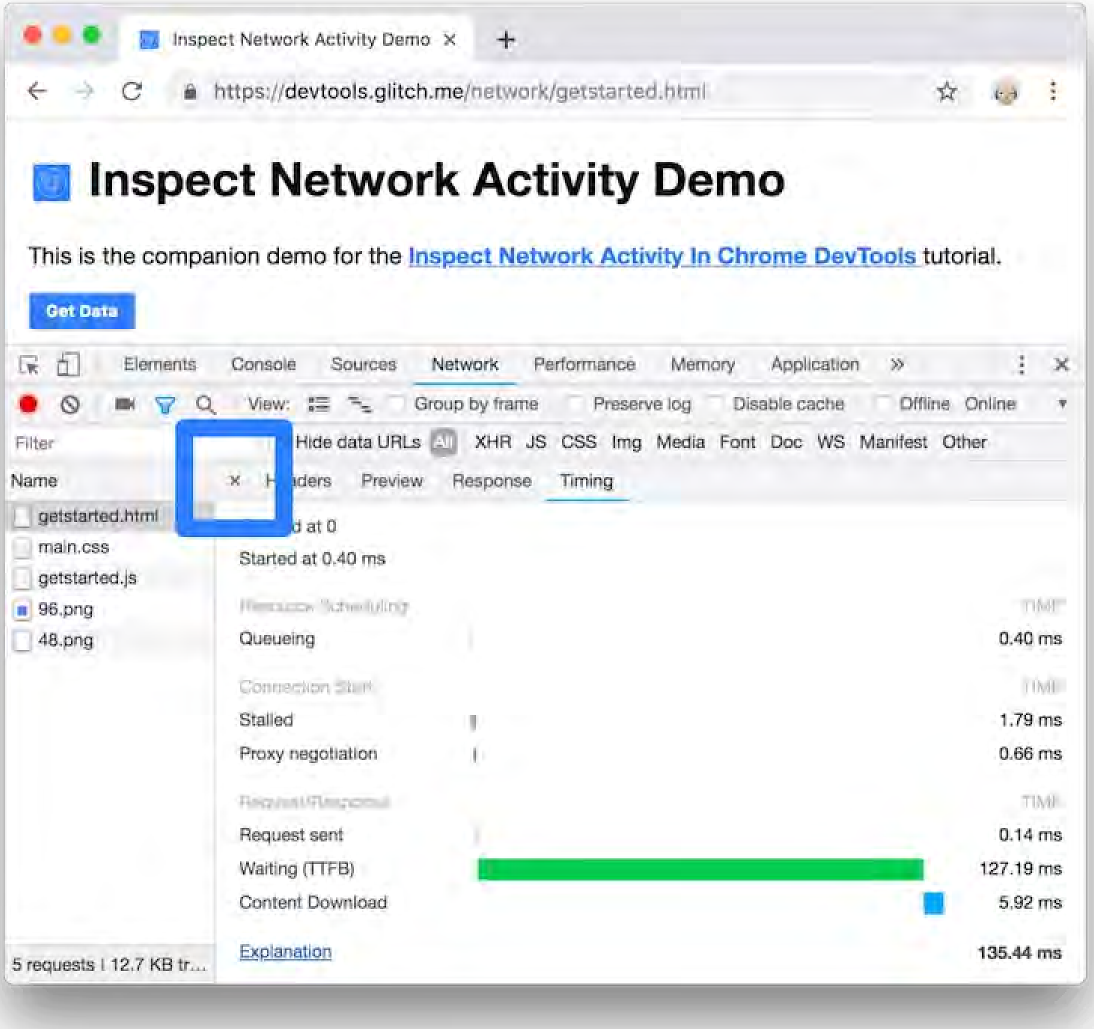
Get Data

Queued at 0
Started at 0.40 ms

Resource Scheduling	TIME
Queueing	0.40 ms
Connection Start	**TIME**
Stalled	1.79 ms
Proxy negotiation	0.66 ms
Request/Response	**TIME**
Request sent	0.14 ms
Waiting (TTFB)	127.19 ms
Content Download	5.92 ms
Explanation	135.44 ms

Figure 17. The Timing tab

5 Click **Close** ✕ to view the Network Log again.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

d at 0

Started at 0.40 ms

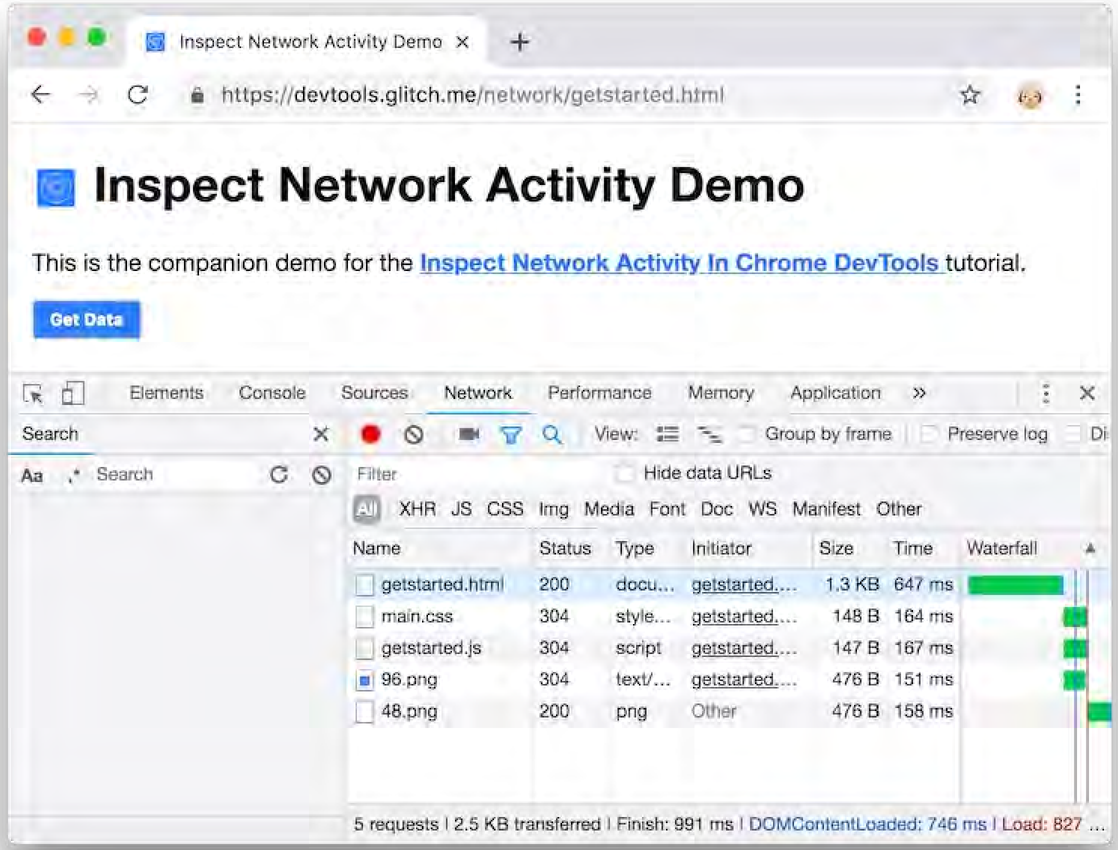
Resource Scheduling	TIME
Queueing	0.40 ms
Connection Start	TIME
Stalled	1.79 ms
Proxy negotiation	0.66 ms
Request/Response	TIME
Request sent	0.14 ms
Waiting (TTFB)	127.19 ms
Content Download	5.92 ms
Explanation	135.44 ms

Figure 18. The Close button

Search network headers and responses

Use the **Search** pane when you need to search the HTTP headers and responses of all resources for a certain string or regular expression.

For example, suppose you want to check if your resources are using reasonable cache policies.

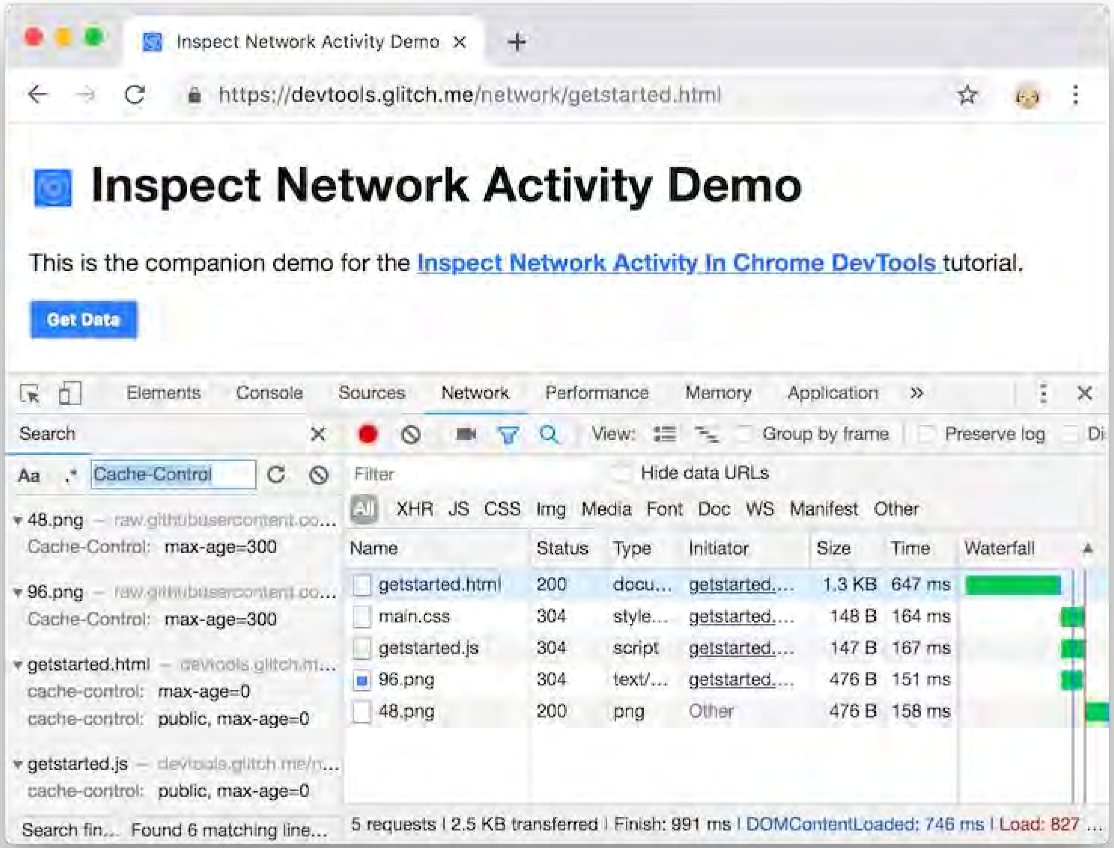

Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Inspect Network Activity Demo
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.
Get Data
Elements
Console
Sources
Network
Performance
Memory
Application
Search
View:
Group by frame
Preserve log
Aa
Search
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docu...	getstarted....	1.3 KB	647 ms	
main.css	304	style...	getstarted....	148 B	164 ms	
getstarted.js	304	script	getstarted....	147 B	167 ms	
96.png	304	text/...	getstarted....	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ...

Figure 19. The Search pane

2 Type `Cache-Control` and press Enter. The Search pane lists all instances of `Cache-Control` that it finds in resource headers or content.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

▾ 48.png — raw.githubusercontent.co…
Cache-Control: max-age=300

▾ 96.png — raw.githubusercontent.co…
Cache-Control: max-age=300

▾ getstarted.html — devtools.glitch.m…
cache-control: max-age=0
cache-control: public, max-age=0

▾ getstarted.js — devtools.glitch.me/n…
cache-control: public, max-age=0

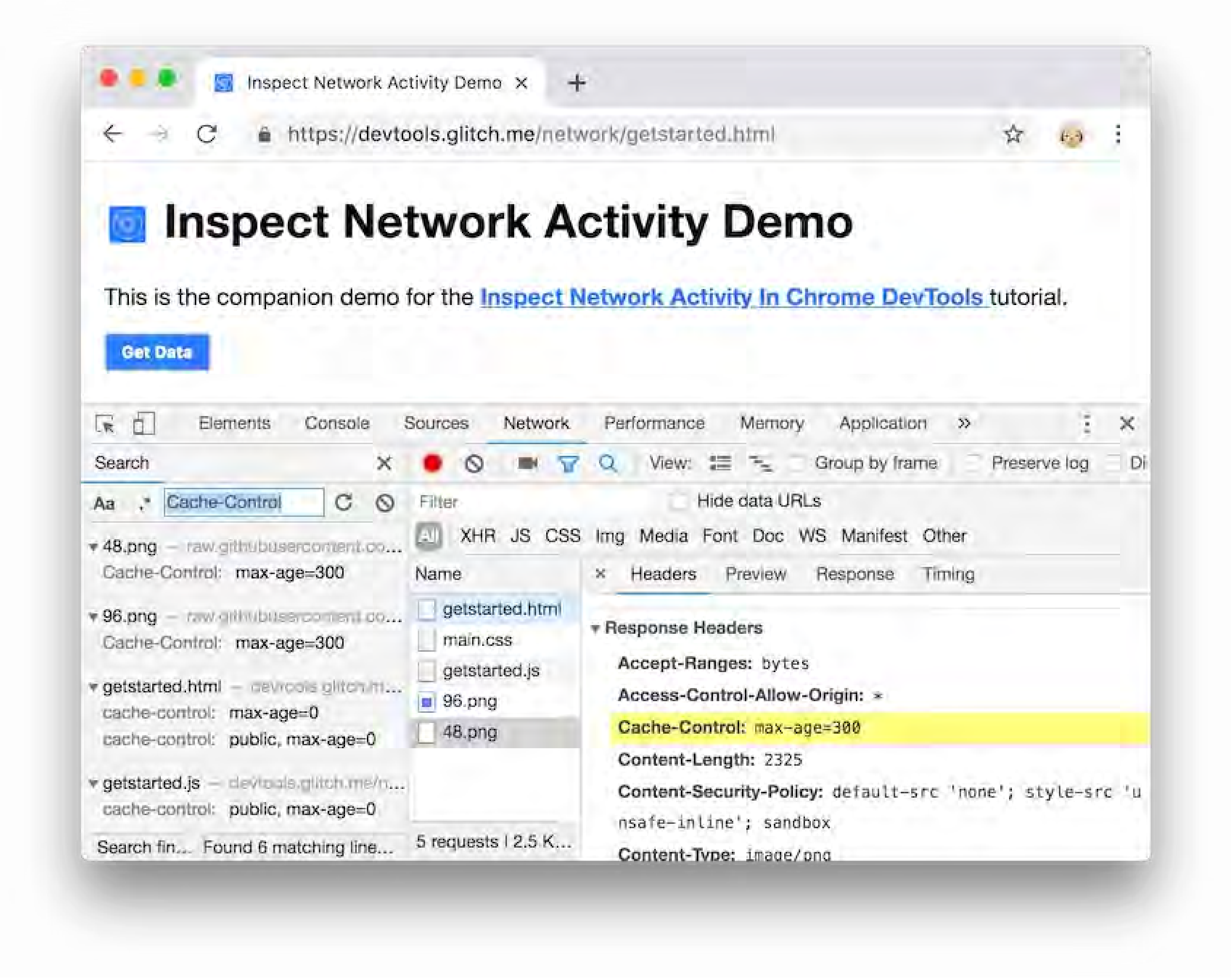
Search fin… Found 6 matching line…

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	docu…	getstarted.…	1.3 KB	647 ms	
main.css	304	style…	getstarted.…	148 B	164 ms	
getstarted.js	304	script	getstarted.…	147 B	167 ms	
96.png	304	text/…	getstarted.…	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 …

Figure 20. Search results for `Cache-Control`

3 Click a result to view it. If the query was found in a header, the Headers tab opens. If the query was found in content, the Response tab opens.



Inspect Network Activity Demo

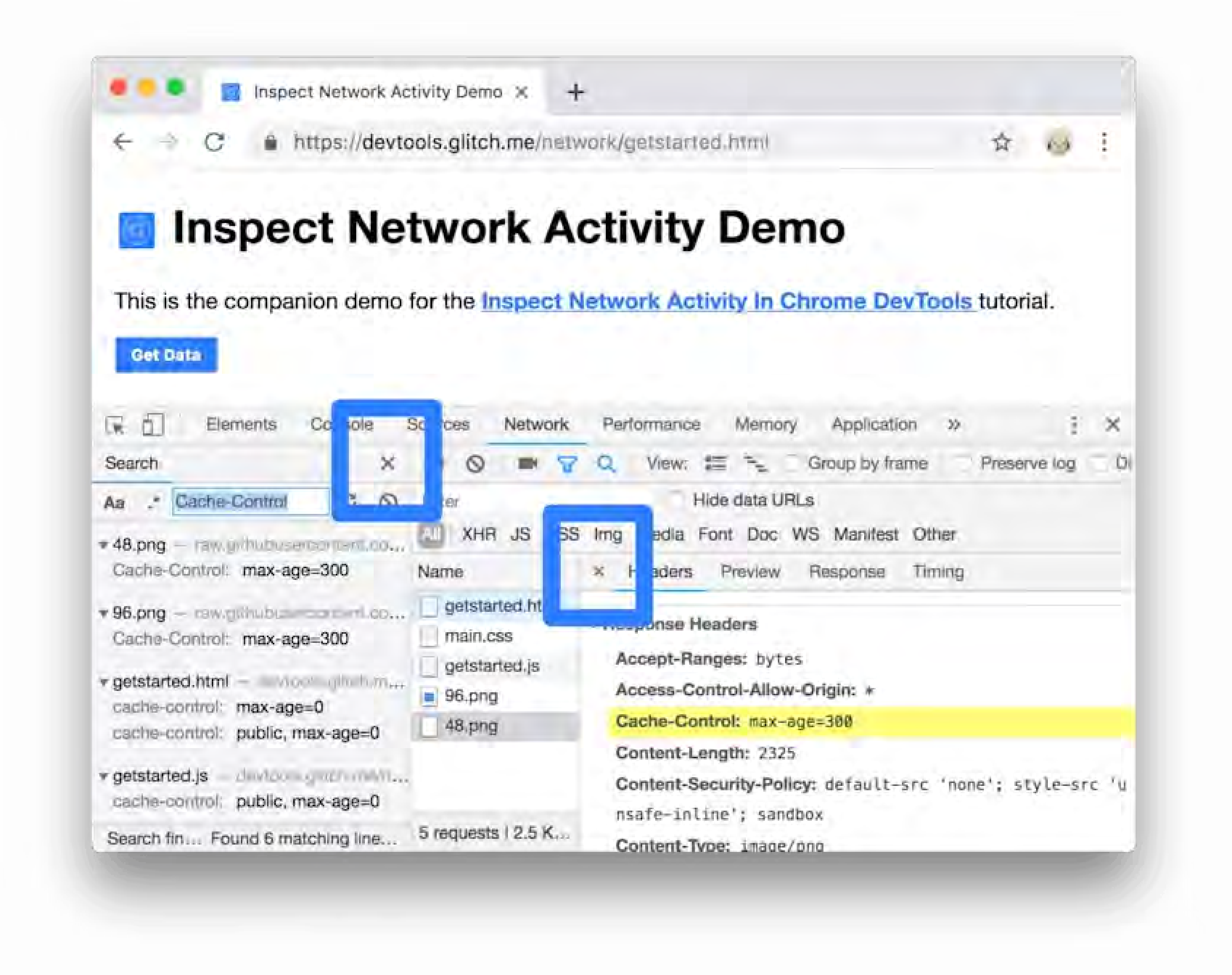
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

```
▾ 48.png — raw.githubusercontent.co…
    Cache-Control:  max-age=300
▾ 96.png — raw.githubusercontent.co…
    Cache-Control:  max-age=300
▾ getstarted.html — devtools.glitch.m…
    cache-control:  max-age=0
    cache-control:  public, max-age=0
▾ getstarted.js — devtools.glitch.me/n…
    cache-control:  public, max-age=0
```

```
▾ Response Headers
    Accept-Ranges: bytes
    Access-Control-Allow-Origin: *
    Cache-Control: max-age=300
    Content-Length: 2325
    Content-Security-Policy: default-src 'none'; style-src 'u
    nsafe-inline'; sandbox
    Content-Type: image/png
```

Figure 21. A search result highlighted in the Headers tab

4 Close the Search pane and the Timing tab.



https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

48.png — raw.githubusercontent.co...
Cache-Control: max-age=300

96.png — raw.githubusercontent.co...
Cache-Control: max-age=300

getstarted.html — devtools.glitch.m...
cache-control: max-age=0
cache-control: public, max-age=0

getstarted.js — devtools.glitch.me/n...
cache-control: public, max-age=0

Search fin... Found 6 matching line...

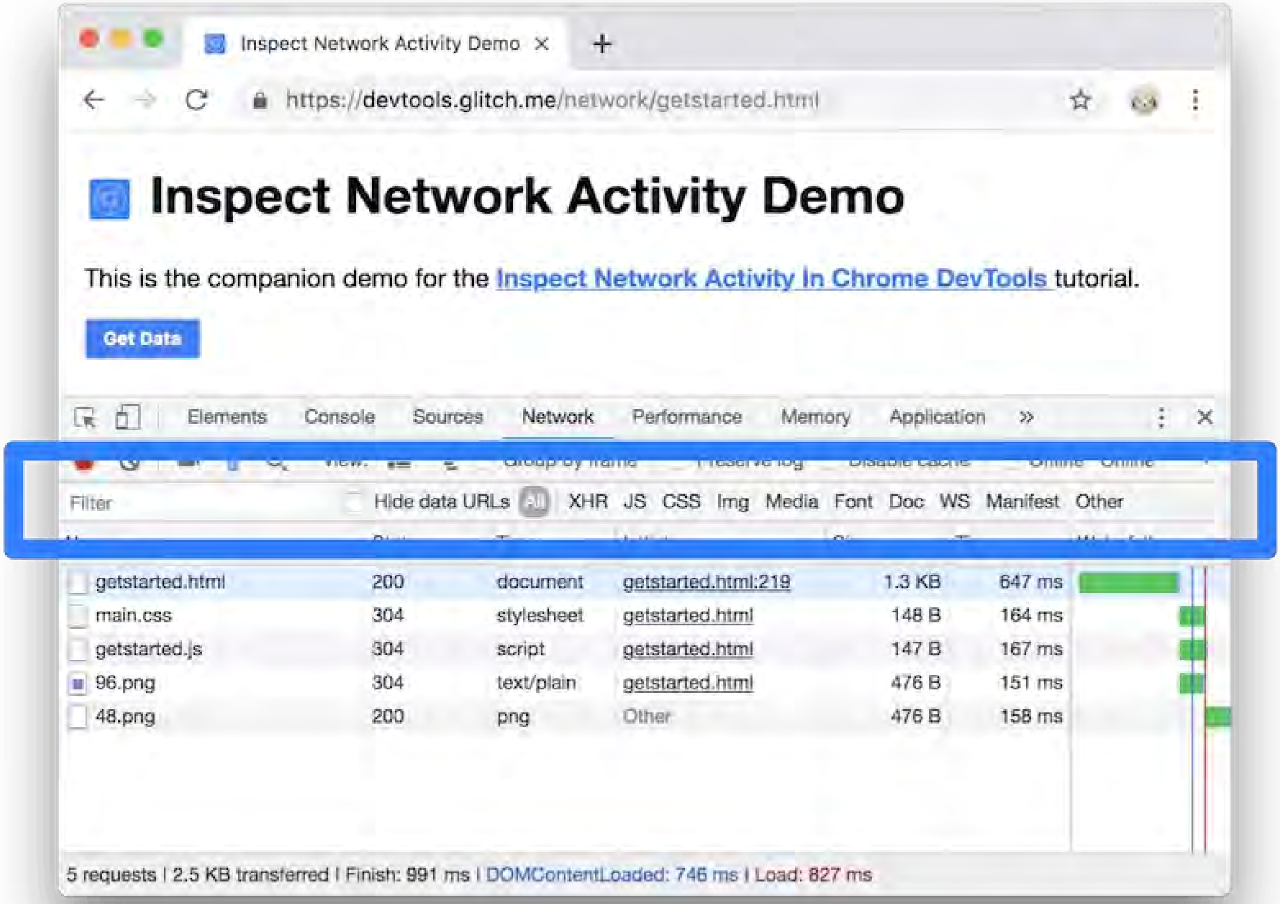
5 requests | 2.5 K...

```
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: max-age=300
Content-Length: 2325
Content-Security-Policy: default-src 'none'; style-src 'u
nsafe-inline'; sandbox
Content-Type: image/png
```

Figure 22. The Close buttons

Filter resources

DevTools provides numerous workflows for filtering out resources that aren't relevant to the task at hand.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

getstarted.html	200	document	getstarted.html:219	1.3 KB	647 ms
main.css	304	stylesheet	getstarted.html	148 B	164 ms
getstarted.js	304	script	getstarted.html	147 B	167 ms
96.png	304	text/plain	getstarted.html	476 B	151 ms
48.png	200	png	Other	476 B	158 ms

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

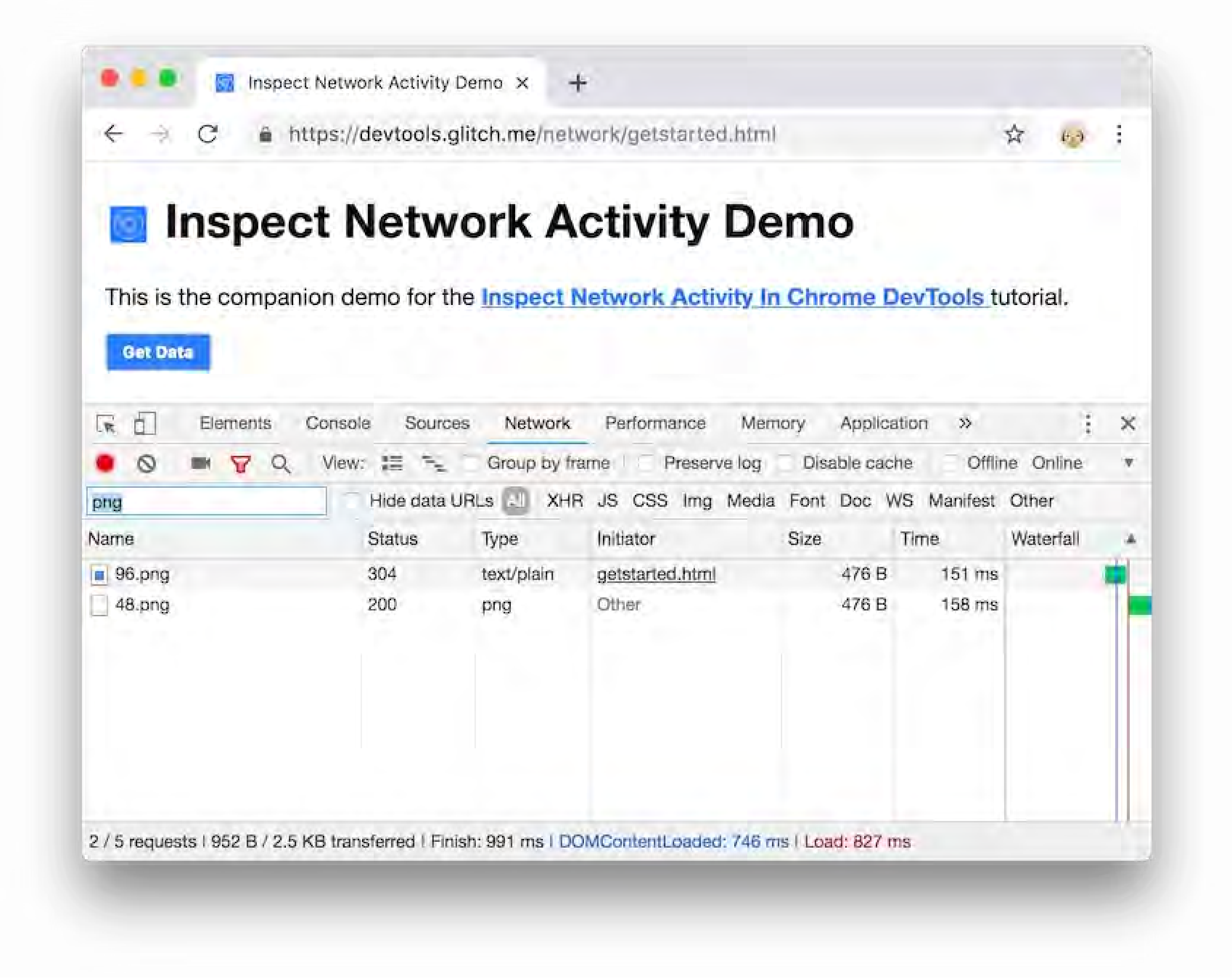
Figure 23. The Filters toolbar

The **Filters** toolbar should be enabled by default. If not:

1 Click **Filter** to show it.

Filter by string, regular expression, or property

The **Filter** text box supports many different types of filtering.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

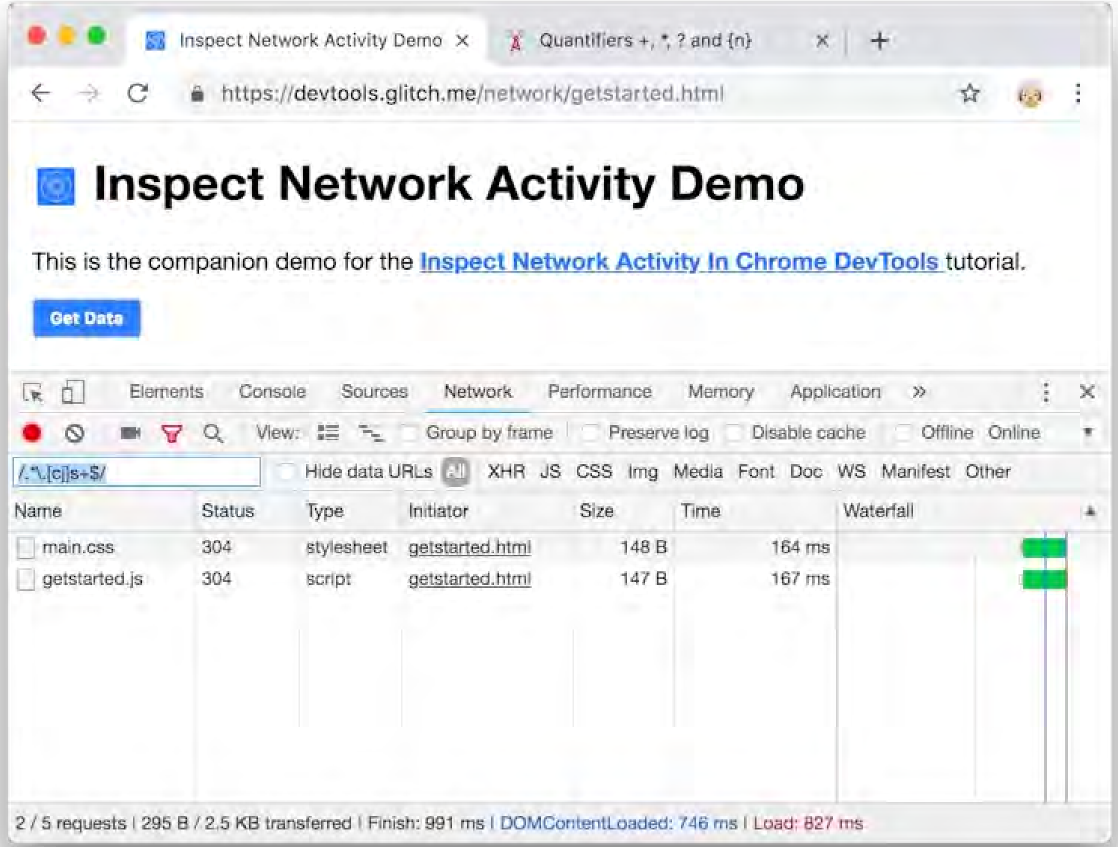
Filter: png

Name	Status	Type	Initiator	Size	Time
96.png	304	text/plain	getstarted.html	476 B	151 ms
48.png	200	png	Other	476 B	158 ms

2 / 5 requests | 952 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 24. A string filter

2 Type `/.*\.[cj]s+$/`. DevTools filters out any resource with a filename that doesn't end with a `j` or a `c` followed by 1 or more `s` characters.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

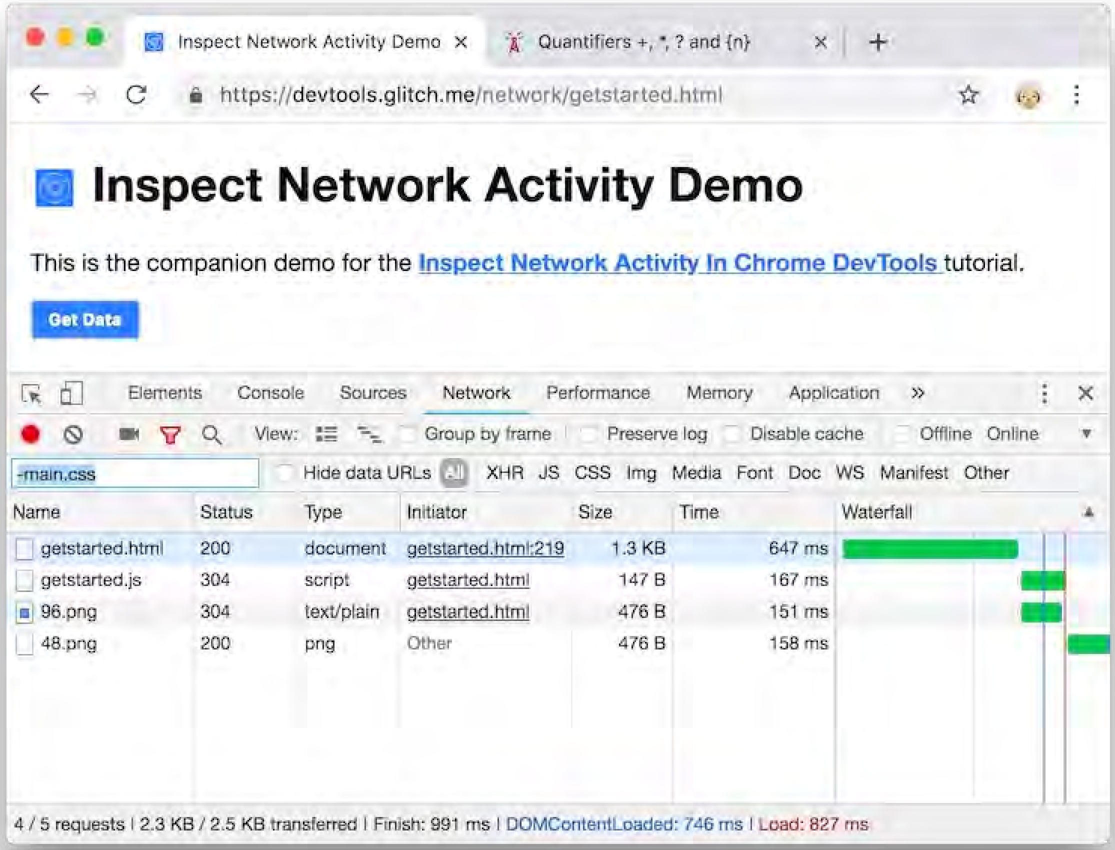
/.*\.[cj]s+$/

Name	Status	Type	Initiator	Size	Time
main.css	304	stylesheet	getstarted.html	148 B	164 ms
getstarted.js	304	script	getstarted.html	147 B	167 ms

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 25. A regular expression filter

3 Type `-main.css`. DevTools filters out `main.css`. If any other file matched the pattern they would also be filtered out.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

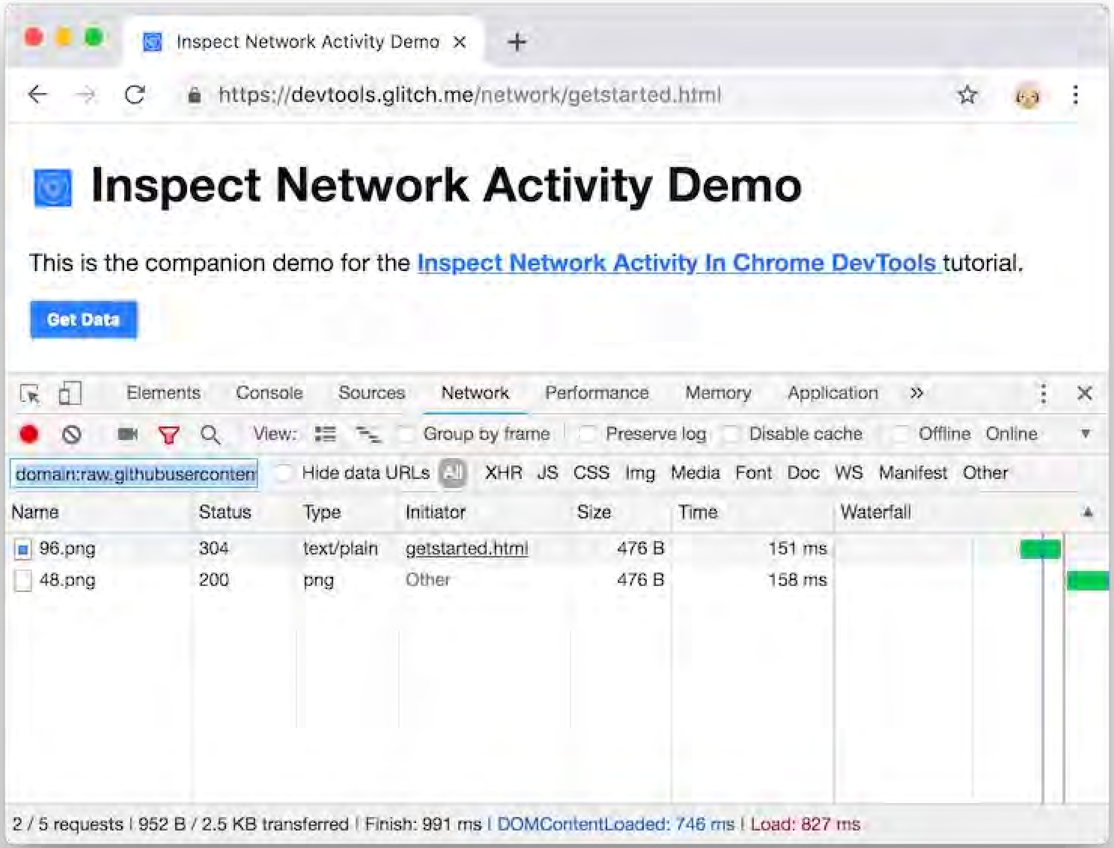
-main.css

Name	Status	Type	Initiator	Size	Time
getstarted.html	200	document	getstarted.html:219	1.3 KB	647 ms
getstarted.js	304	script	getstarted.html	147 B	167 ms
96.png	304	text/plain	getstarted.html	476 B	151 ms
48.png	200	png	Other	476 B	158 ms

4 / 5 requests | 2.3 KB / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 26. A negative filter

4 Type `domain:raw.githubusercontent.com` into the **Filter** text box. DevTools filters out any resource with a URL that does not match this domain.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

domain:raw.githubuserconten

Name	Status	Type	Initiator	Size	Time	Waterfall
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

2 / 5 requests | 952 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 27. A property filter

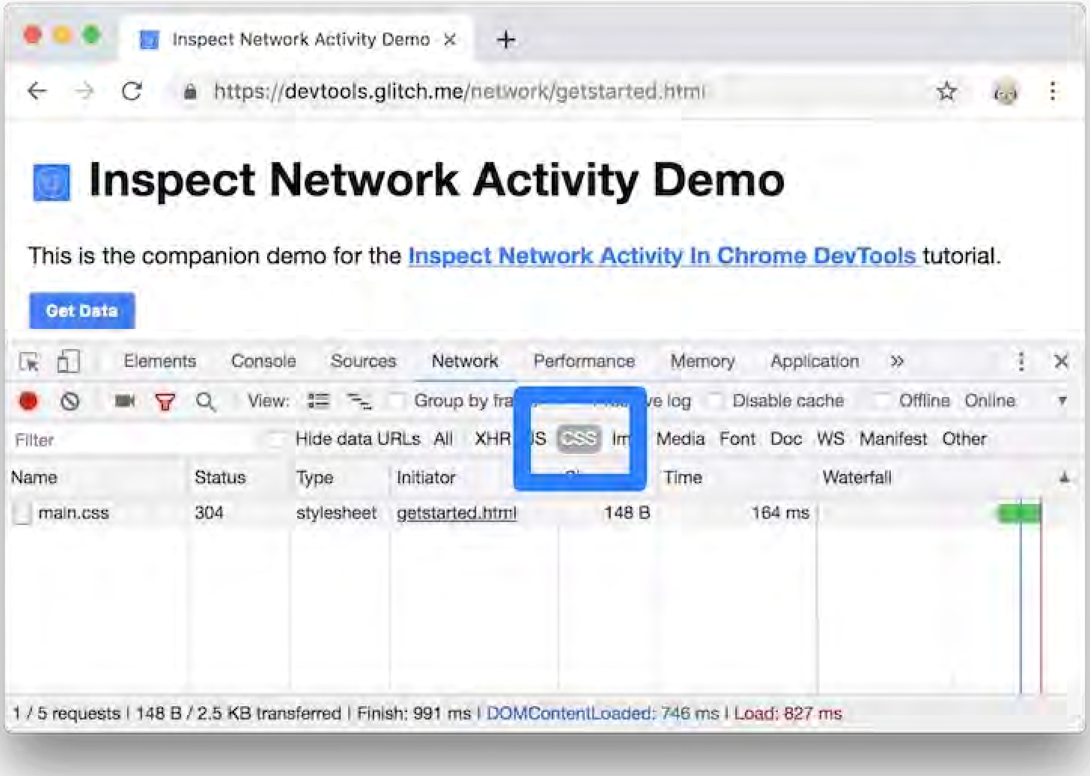
See Filter requests by properties for the full list of filterable properties.

5 Clear the **Filter** text box of any text.

Filter by resource type

To focus in on a certain type of file, such as stylesheets:

1 Click **CSS**. All other file types are filtered out.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

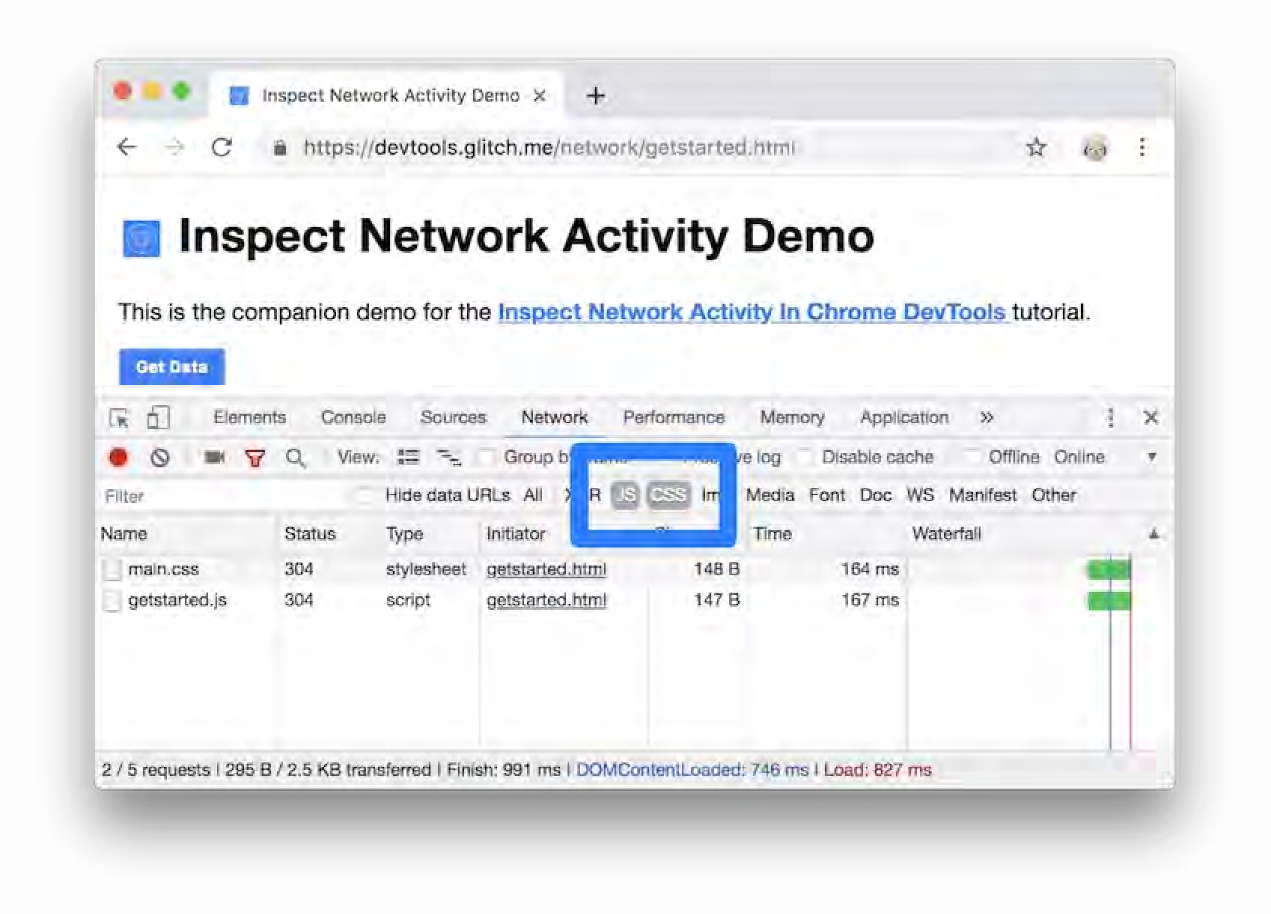
Get Data

Name	Status	Type	Initiator		Time	Waterfall
main.css	304	stylesheet	getstarted.html	148 B	164 ms	

1 / 5 requests | 148 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 28. Showing CSS files only

2 To also see scripts, hold Control or Command (Mac) and then click **JS**.



https://devtools.glitch.me/network/getstarted.html

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Get Data

Name	Status	Type	Initiator		Time	Waterfall
main.css	304	stylesheet	getstarted.html	148 B	164 ms	
getstarted.js	304	script	getstarted.html	147 B	167 ms	

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 29. Showing CSS and JS files only

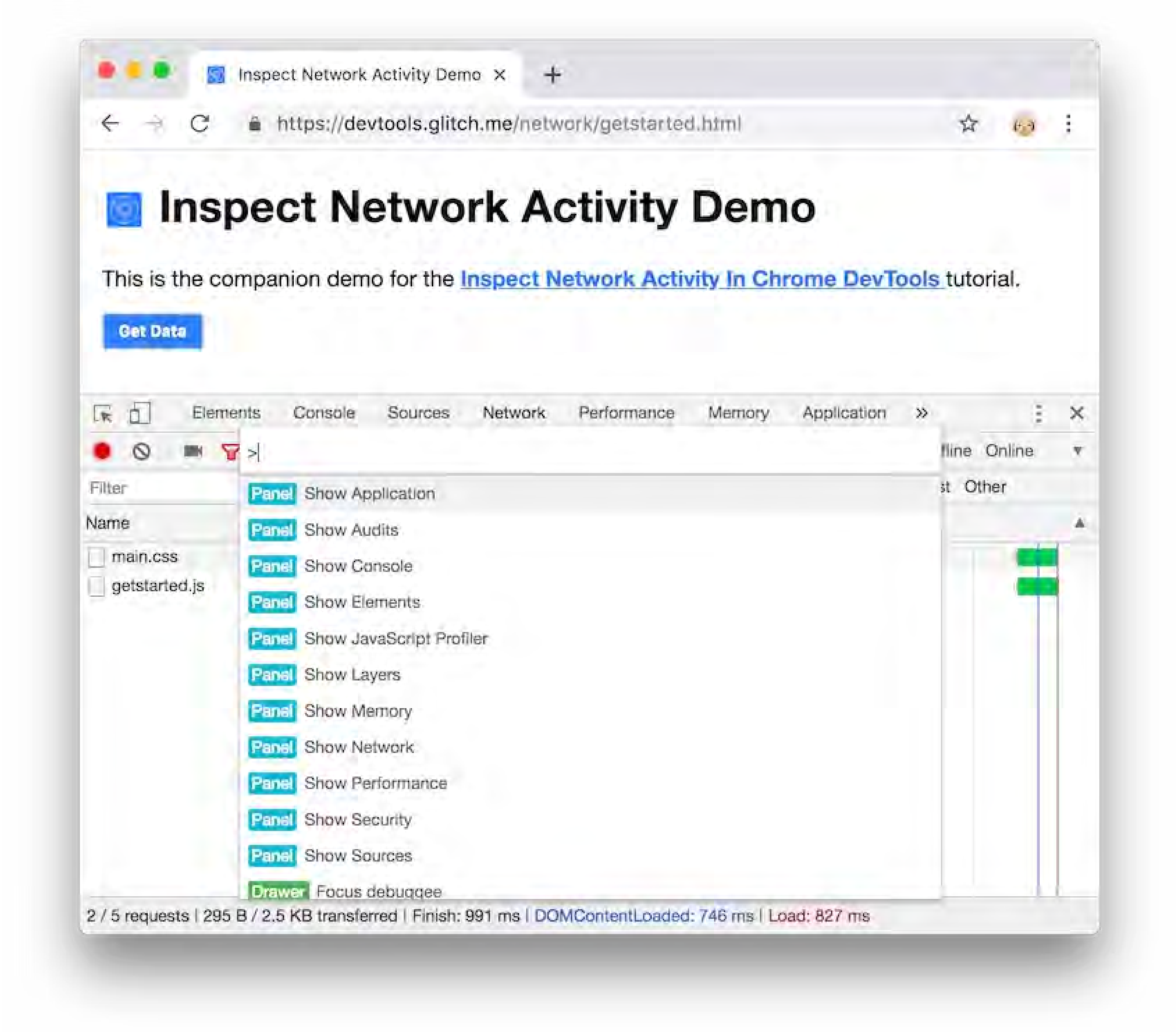
3 Click **All** to remove the filters and see all resources again.

See Filter requests for other filtering workflows.

Block requests

How does a page look and behave when some of its resources aren't available? Does it fail completely, or is it still somewhat functional? Block requests to find out:

1 Press Control+Shift+P or Command+Shift+P (Mac) to open the **Command Menu**.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 30. The Command Menu

2 Type `block`, select **Show Request Blocking**, and press Enter.

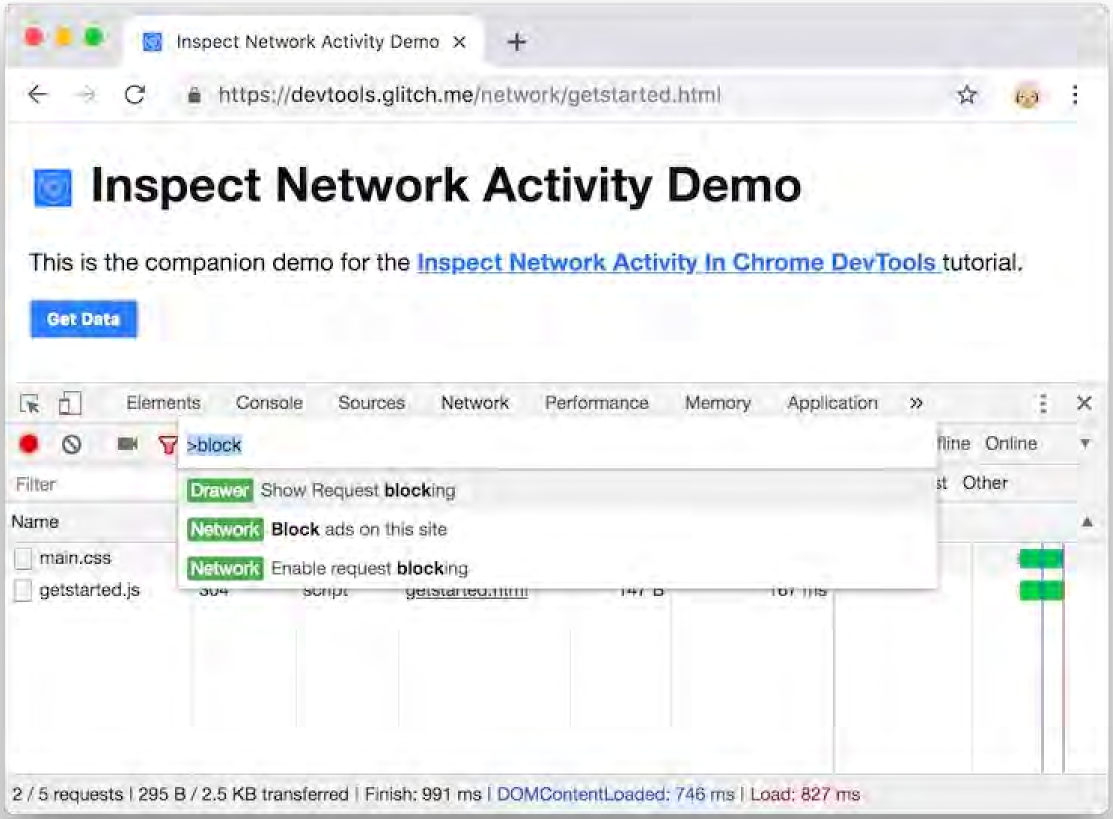
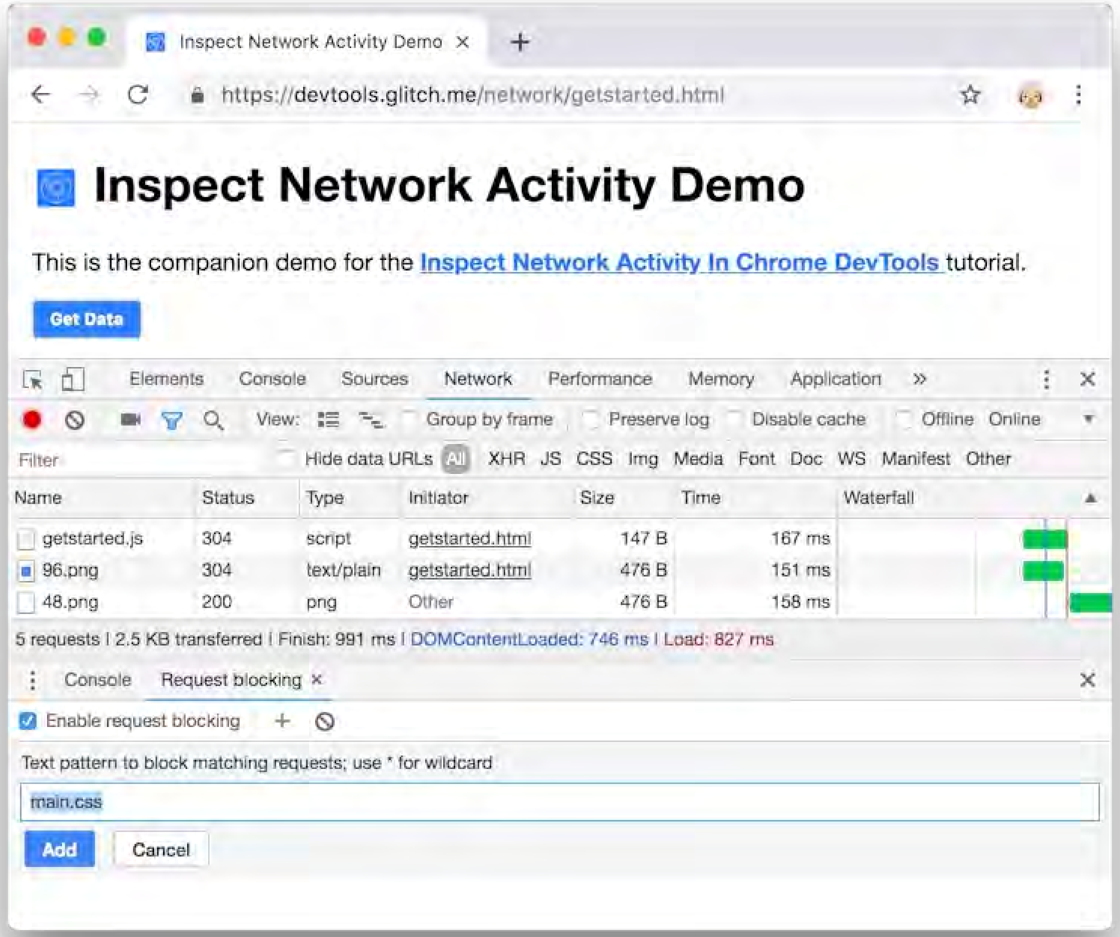

Inspect Network Activity Demo
https://devtools.glitch.me/network/getstarted.html
Inspect Network Activity Demo
This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.
Get Data
Elements
Console
Sources
Network
Performance
Memory
Application
>block
Drawer Show Request blocking
Network Block ads on this site
Network Enable request blocking
Filter
Name
main.css
getstarted.js
Online
Other
2 / 5 requests | 295 B / 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

Figure 31. Show Request Blocking

3 Click **Add Pattern** ＋.

4 Type `main.css`.



Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.js	304	script	getstarted.html	147 B	167 ms	
96.png	304	text/plain	getstarted.html	476 B	151 ms	
48.png	200	png	Other	476 B	158 ms	

5 requests | 2.5 KB transferred | Finish: 991 ms | DOMContentLoaded: 746 ms | Load: 827 ms

☑ Enable request blocking

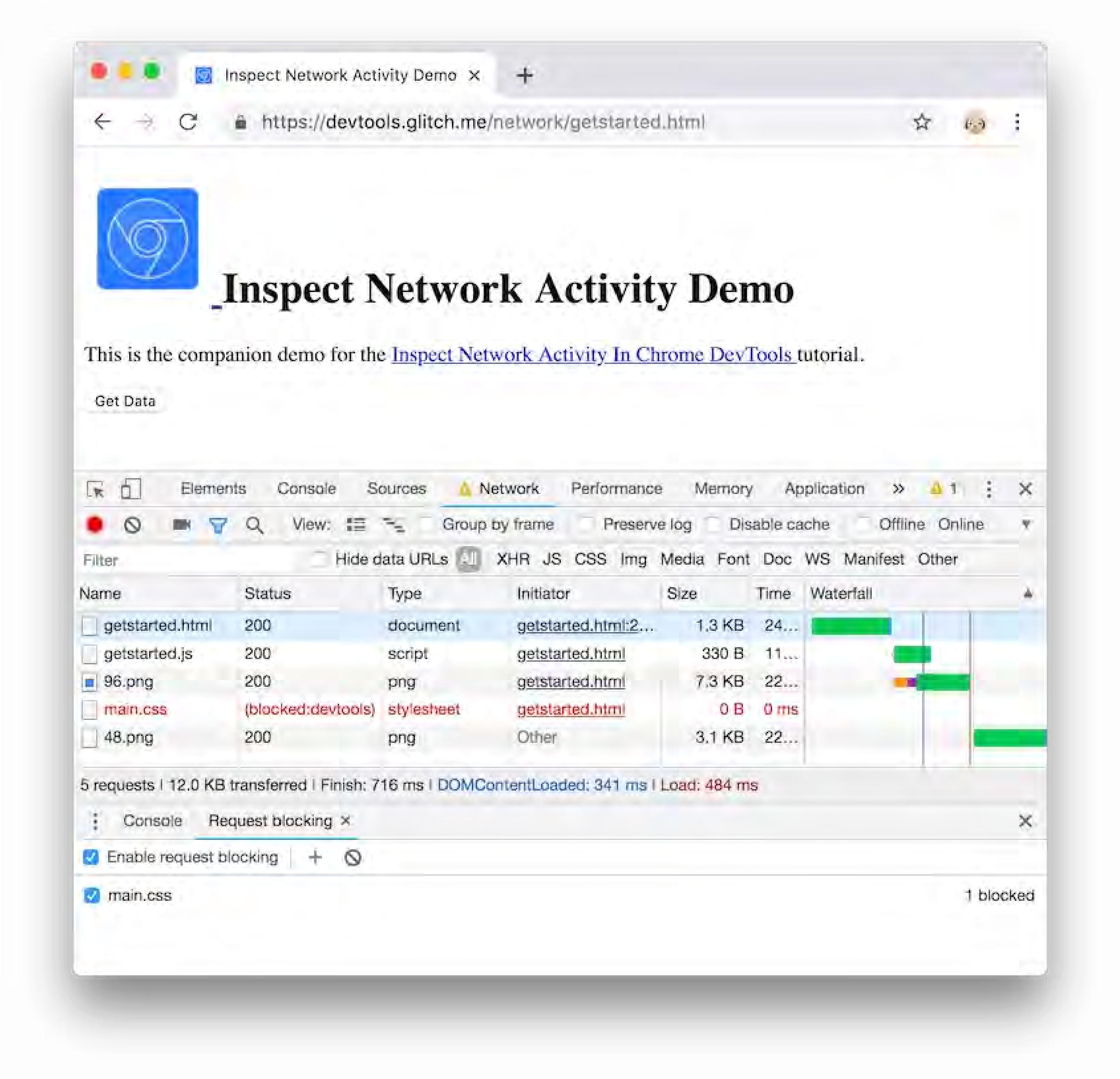
Text pattern to block matching requests; use * for wildcard

main.css

Figure 32. Blocking `main.css`

5 Click **Add**.

6 Reload the page. As expected, the page's styling is slightly messed up because its main stylesheet has been blocked. Note the `main.css` row in the Network Log. The red text means that the resource was blocked.


Inspect Network Activity Demo ×
https://devtools.glitch.me/network/getstarted.html
Get Data
Elements
Console
Sources
Network
Performance
Memory
Application
View:
Filter
XHR JS CSS Img Media Font Doc WS Manifest Other
Console
Request blocking ×

Inspect Network Activity Demo

This is the companion demo for the Inspect Network Activity In Chrome DevTools tutorial.

□ Group by frame □ Preserve log □ Disable cache □ Offline Online

□ Hide data URLs All

Name	Status	Type	Initiator	Size	Time	Waterfall
getstarted.html	200	document	getstarted.html:2…	1.3 KB	24…	
getstarted.js	200	script	getstarted.html	330 B	11…	
96.png	200	png	getstarted.html	7.3 KB	22…	
main.css	(blocked:devtools)	stylesheet	getstarted.html	0 B	0 ms	
48.png	200	png	Other	3.1 KB	22…	

5 requests | 12.0 KB transferred | Finish: 716 ms | DOMContentLoaded: 341 ms | Load: 484 ms

☑ Enable request blocking

☑ main.css 1 blocked

Figure 33. `main.css` has been blocked

7 Uncheck the **Enable request blocking** checkbox.

Next steps

Congratulations, you have completed the tutorial. Click **Dispense Award** to receive your award.

Follow us

Contribute

File a bug

View source

Related content

web.dev

Case studies

Podcasts

Connect

Twitter

YouTube

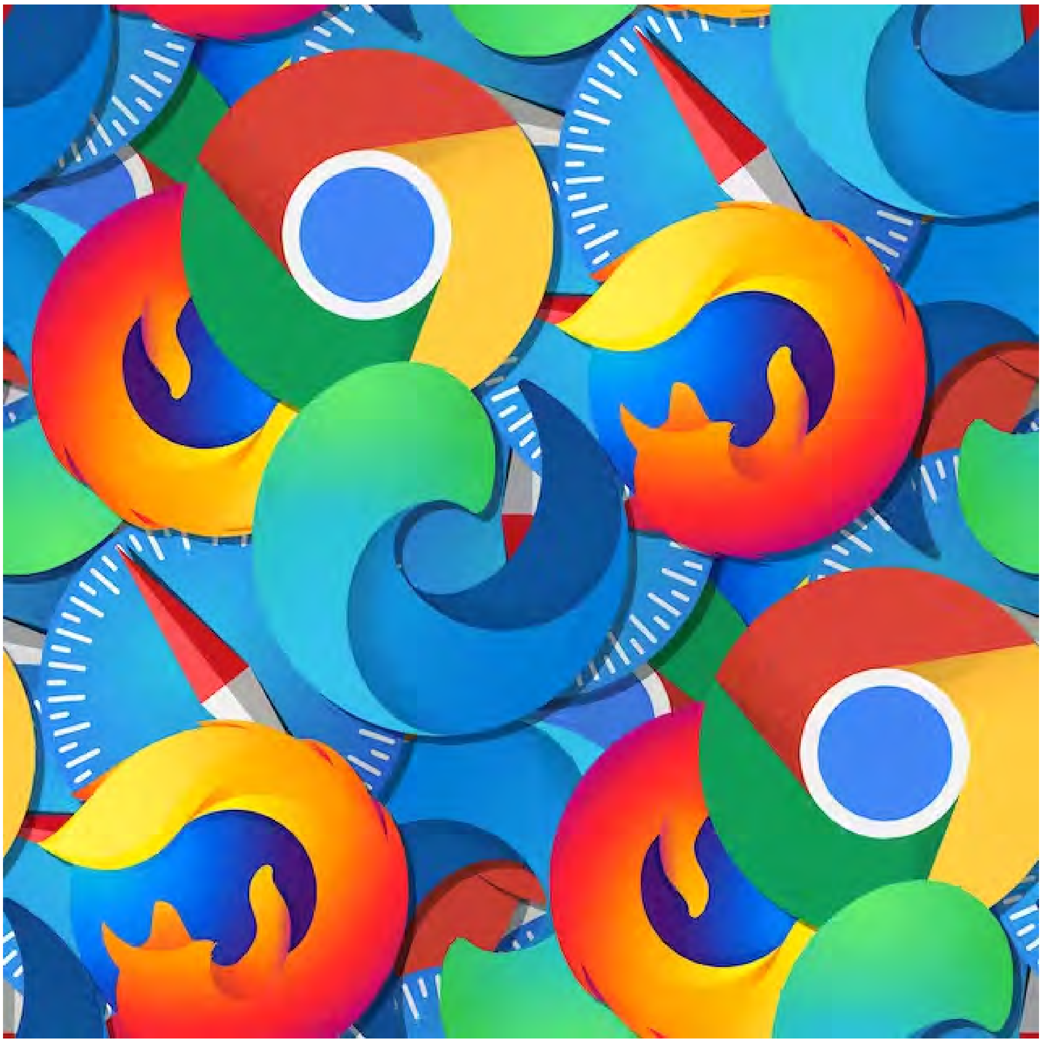
GitHub

Google for Developers

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #526

THE CONVERSATION

Academic rigor, journalistic flair



The major browsers have privacy modes, but don’t confuse privacy for anonymity. Oleg Mishutin/iStock via Getty Images

Private browsing: What it does – and doesn’t do – to shield you from prying eyes on the web

Published: July 30, 2020 8.10am EDT

Lorrie Cranor

Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University

Hana Habib

Graduate Research Assistant at the Institute for Software Research, Carnegie Mellon University

Languages

Español

English

Leer en español

Many people look for more privacy when they browse the web by using their browsers in privacy-protecting modes, called “Private Browsing” in Mozilla Firefox, Opera and Apple Safari; “Incognito” in Google Chrome; and “InPrivate” in Microsoft Edge.

These private browsing tools sound reassuring, and they’re popular. According to a 2017 survey, nearly half of American internet users have tried a private browsing mode, and most who have tried it use it regularly.

However, our research has found that many people who use private browsing have misconceptions about what protection they’re gaining. A common misconception is that these browser modes allow you to browse the web anonymously, surfing the web without websites identifying you and without your internet service provider or your employer knowing what websites you visit. The tools actually provide much more limited protections.

Other studies conducted by the Pew Research Center and the privacy-protective search engine company DuckDuckGo have similar findings. In fact, a recent lawsuit against Google alleges that internet users are not getting the privacy protection they expect when using Chrome’s Incognito mode.

How it works

While the exact implementation varies from browser to browser, what private browsing modes have in common is that once you close your private browsing window, your browser no longer stores the websites you visited, cookies, user names, passwords and information from forms you filled out during that private browsing session.

Essentially, each time you open a new private browsing window you are given a “clean slate” in the form of a brand new browser window that has not stored any browsing history or cookies. When you close your private browsing window, the slate is wiped clean again and the browsing history and cookies from that private browsing session are deleted. However, if you bookmark a site or download a file while using private browsing mode, the bookmarks and file will remain on your system.

Although some browsers, including Safari and Firefox, offer some additional protection against web trackers, private browsing mode does not guarantee that your web activities cannot be linked back to you or your device. Notably, private browsing mode does not prevent websites from learning your internet address, and it does not prevent your employer, school or internet service provider from seeing your web activities by tracking your IP address.

Reasons to use it

We conducted a research study in which we identified reasons people use private browsing mode. Most study participants wanted to protect their browsing activities or personal data from other users of their devices. Private browsing is actually pretty effective for this purpose.

We found that people often used private browsing to visit websites or conduct searches that they did not want other users of their device to see, such as those that might be embarrassing or related to a surprise gift. In addition, private browsing is an easy way to log out of websites when borrowing someone else's device – so long as you remember to close the window when you are done.

Smart phone displaying Google incognito mode

Private browsing can help cover your internet tracks by automatically deleting your browsing history and cookies when you close the browser. Avishek Das/SOPA Images/LightRocket via Getty Images

Private browsing provides some protection against cookie-based tracking. Since cookies from your private browsing session are not stored after you close your private browsing window, it's less likely that you will see online advertising in the future related to the websites you visit while using private browsing.

[*Get the best of The Conversation, every weekend.* Sign up for our weekly newsletter.]

Additionally, as long as you have not logged into your Google account, any searches you make will not appear in your Google account history and will not affect future Google search results. Similarly, if you watch a video on YouTube or other service in private browsing, as long as you are not logged into that service, your activity does not affect the recommendations you get in normal browsing mode.

What it doesn't do

Private browsing does not make you anonymous online. Anyone who can see your internet traffic – your school or employer, your internet service provider, government agencies, people snooping on your public wireless connection – can see your browsing activity. Shielding that activity requires more sophisticated tools that use encryption, like virtual private networks.

Private browsing also offers few security protections. In particular, it does not prevent you from downloading a virus or malware to your device. Additionally, private browsing does not offer any additional protection for the transmission of your credit card or other personal information to a website when you fill out an online form.

It is also important to note that the longer you leave your private browsing window open, the more browsing data and cookies it accumulates, reducing your privacy protection. Therefore, you should get in the habit of closing your private browsing window frequently to wipe your slate clean.

What's in a name

It is not all that surprising that people have misconceptions about how private browsing mode works; the word "private" suggests a lot more protection than these modes actually provide.

Furthermore, a 2018 research study found that the disclosures shown on the landing pages of private browsing windows do little to dispel misconceptions that people have about these modes. Chrome provides more information about what is and is not protected than most of the other browsers, and Mozilla now links to an informational page on the common myths related to private browsing.

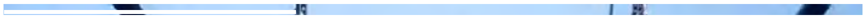
However, it may be difficult to dispel all of these myths without changing the name of the browsing mode and making it clear that private browsing stops your browser from keeping a record of your browsing activity, but it isn't a comprehensive privacy shield.

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #700

By Khamosh Pathak Published October 10, 2014

6681037203 9257782E8A Z

Many internet users think that incognito mode in Google Chrome is like a magical cloak that will instantly gives them internet privacy. That's just not true.



You can use Chrome to play some of the common audio and video file formats.

Incognito mode gets a bad rep. Some say it's only used to hide "indecent" behavior. But there are legitimate uses for it. What is incognito mode? Just how "private" is it? Why even use it? And is there anything better to keep your affairs private on the internet? All of your questions will be answered below.

1. IT'S NOT REALLY PRIVATE

Well, **nothing** really is private these days but if you're thinking that switching to incognito mode is going to magically cloak your internet behavior, you're wrong.

When you switch to the incognito tab, Chrome itself tells you, “Going incognito **doesn’t** hide your browsing from your employer, your internet service provider, or the websites you visit.”

right behind you.

2. IT WON’T SAVE YOU FROM SECRET AGENTS

Before the NSA revelations and the incognito page redesign, Chrome had a funny line in there. Thanks to Dailykos we can all enjoy it. Listed under *Be wary of* was **Surveillance by secret agents**.

Top 11 Red Dead Redemption 2 Wallpapers in 4K and Full HD

How to Connect Steam to Discord and What to Do if You Can’t

Image capture via Dailykos.

That little joke turned out to be a little too true and was consequently removed from the redesign.

The point I'm trying to make is that when it comes to privacy, incognito mode is certainly not what you should be relying upon.

3. INCOGNITO MODE: WHAT IS IT GOOD FOR?

The point of incognito mode is not to hide your identity from the rest of the world, it's to hide your interactions with the internet from the PC you're using (and the Google account you're logged into).

Cool Tip: If you're letting a friend check their email or log into Facebook on your can use your computer without having all of their user information saved in your cookies, and you don't have to relog into all of your sites.

When you use incognito mode, Chrome doesn't record any history or cookies, and it disables browser extensions. This means that third party services like Facebook, Google, etc that use cookies to track your movement across the internet to serve you better ads won't follow you to the incognito tab.

Due to these reasons, incognito mode is generally safer when making banking transactions or having conversations you don't want to be recorded **on your PC**.

> *When cookies and extensions are disabled, the chances of a malicious app stealing your data are largely reduced.*

If you use Gmail, Google Search and an Android phone, you know just how obsessive Google's tracking is. Google Now on your phone will follow up on something you searched for on a computer that one time. Incognito mode prevents such encounters.

4. IS THERE A WAY TO TRULY BE PRIVATE ON THE INTERNET?

VPN Maybe

Maybe not "truly" (ahem, secret agents), but we can surely try. Using VPN is usually the easiest and most effective way. A VPN **masks** physical location and IP address. So the website you're visiting doesn't really know who or where you are.

Chrome has two good VPN extensions called ZenMate and Hola. I've written about security based extensions on Chrome in detail before.

For Windows and mobile devices, Hotspot Shield and TunnelBear are great VPN services.

But if you really do not want to take any chances when it comes to privacy, you can check out VPN services like NordVPN and ExpressVPN (sign up using this link and save 49% on a yearly ExpressVPN plan.)

Use Tor Instead of Chrome

Chrome is built by Google. It is arguably the fastest and most feature rich browser out there. But Google makes money by serving you ads based on your personal information. By using anything from Google you're essentially giving up your privacy.

To a lot of people, that's worth the convenience.

If you really want to say no to Chrome, try Tor as your browser. It's an open source browser that's designed from the ground up to hide the identity of the user. It works similar to VPN software but on a browser level.

WHAT DO YOU USE THE INCOGNITO MODE FOR?

Let us know what you use incognito mode for in the comments below, but please, don't be indecent!

Top image via Normand Desjardins

Last updated on 03 February, 2022

The above article may contain affiliate links which help support Guiding Tech. However, it does not affect our editorial integrity. The content remains unbiased and authentic.

Read Next

Instantly Switch a Chrome Tab to Incognito (Private) Mode

Private browsing has its uses – from public computers to even the ones in your house if you have more than one person sharing a computer.

Private Browsing on Android (or Incognito Mode) – 2 Ways

Whenever you want to go off the records while browsing on a computer, things are easy (I am talking about Firefox, Chrome and Opera users here).

3 Chrome Extensions to Enhance Incognito Mode Experience

Incognito mode is one of the safest ways to browse stuff that we wanna hide from prying eyes.

Enable Extensions in Chrome's Incognito mode

Google Chrome extensions like LastPass, Adblocker and much more are useful tools to enable a smoother experience while browsing but due to security issues, extensions are by default disabled in

Chrome Guest Mode vs Incognito: How Do the Browsing Modes Differ

I'm pretty sure you must have heard about the Incognito mode of the Chrome browser.

✕

How to Always Launch Chrome in Incognito Mode

I have mixed up Incognito mode with normal Chrome windows countless times.

How to Disable Chrome Incognito Mode on Windows, macOS, and

There’s little doubt in regards to the versatility that Chrome’s Incognito mode brings to the table.

What Is Google Maps Incognito Mode and How to Enable It on Your Phone

Google has launched Incognito Mode for Maps, just like what's on Chrome and YouTube.

WRITTEN BY

Khamosh Pathak

See more articles by Khamosh →

Your email address

SUBSCRIBE

#Android
#Windows
#Internet and Social
#iOS
#Gadgets

#How-tos
#Comparisons
#Tips & Tricks

Facebook
Instagram
Instagram (Intl)
YouTube
YouTube (Intl)

Guiding Tech

About
Contact
Terms of Use

#Mac

#Buying Guides

Twitter

Twitter (Intl)

Privacy Policy

Advertise

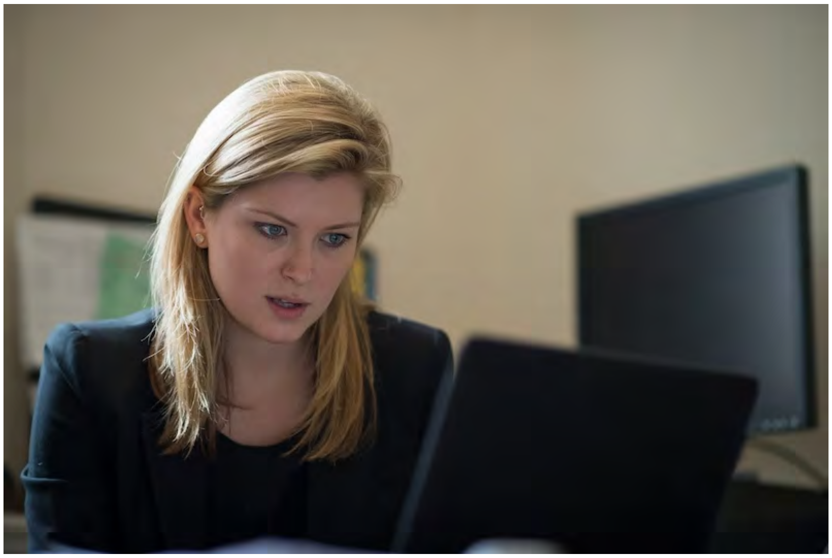
×

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #701

Bustle MENU

Life

These Are All Good Reasons To Use Incognito Mode



LEON NEAL/AFP/Getty Images

by Pamela J. Hobart
Sep. 17, 2016

As most people who browse the internet have noticed by now, most web browser software prominently offers an "incognito mode" option. What is incognito mode anyways, and what are the reasons to use incognito mode? As a recent Reddit thread reveals, there are more than a few.

To understand why you'd want to use private browsing (known as "incognito mode" on the popular browser Chrome), it's best to first understand how incognito mode works. When you open a browser window in private or incognito mode, the browser stops storing all the various stuff it usually stores about sites as you putter around the information superhighway. Typically, this stored stuff includes things like the site's URL, text you may have typed into the site's forms, and cookies from websites (that enable the browser remember your language preference or save your digital shopping cart, for instance). And, very obviously, when you are not in private browsing mode, the browser logs sites you've visited into your "history" log, along with the date and time of the visit.

Bustle

MENU

Incognito mode doesn't offer complete privacy. Your internet service provider still knows where you've browsed, so while incognito mode might hide your searches from your mom, it can't really help you hide from the police and their subpoenas. If someone like your employer is monitoring all of its network's activity from a central location, they'll know where you (or your computer) has navigated, too.

But for personal day-to-day purposes, the incognito mode is really valuable. As explained by the good folks on Reddit, here are some of those times.

1. Looking at porn

This very common incognito mode use case is right there in the question! As everyone knows, internet porn is tremendously popular, but sometimes you want to keep your browsing to yourself. Incognito mode is the answer. You can even conveniently use browsers incognito on your phone.

2. Signing into multiple email accounts at once

You could set up different browser "profiles" to switch between email accounts within one browser, but incognito mode is the quick and easy way of doing this on the fly — no setup required.

3. Watching weird videos

Again, though there is another way to pause videos getting added to your YouTube history (within YouTube settings themselves), the incognito mode is quick and easy.

4. Using computers that aren't yours

If you need to log into your email or your banking account or whatever on a computer away from home, just pop open incognito mode to provide a layer of protection against your passwords or user info being saved to that computer (not totally infallible, that computer could have keystroke logging software on it or something, but it helps).

5. Lame Google searches

Because there's no such thing as a stupid question, except when that old nonsense is staring you down in your autocomplete fields or browser history. Let's send those lame Google searches down the memory hole with incognito mode instead.

6. When you don't want to look like you're up to no good

Some searches just look real bad out of context.

7. Shopping for gifts

Big Data has no reservations about spoiling a surprise. Or "spoiling" a surprise that it not actually about to happen, as it were.

8. Because it's prettier

Ok sure, if you say so!

9. For serious business

The internet definitely isn't all fun and games. People looking for information about divorce, medical conditions, psychological conditions, and the like may want all the privacy they can get.

10. To look like a fresh visitor

If you are tinkering with the code for a website, you may want to prevent your browser from saving ("caching") the site in order to force it to reload the potential changes each time. Also, since Google customizes search results, incognito mode can give you a clean slate of Google search results rather than ones affected by your past Googling.

11. Booking travel

If the airlines are going to play pricing games with us, then we're going to play games with them right back, dammit (though private browsing for a lower fare may or may not actually work).

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #702

Tracking in 'Incognito' or Private Browsing Mode?

FILED UNDER CRASH COURSE ON 22 FEB 2017

It may surprise you that ads can still follow you around in “Incognito” and other “private browsing” modes.

That’s because Incognito mode **isn’t** really private.

😱

content on your computer. Websites, search engines, Internet service providers, and governments can still easily track you across the web.

That's why it's important to use privacy alternatives that don't share your personal information—such as DuckDuckGo for search.

Using Incognito mode to keep you private online is kind of like using a bucket to put out a raging fire:

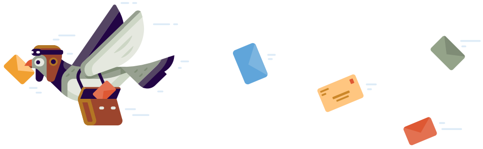
If you didn't know that private browsing isn't private—you're not alone! 67% of people who use private browsing mode over-estimate the protection that private browsing modes offer.

Now you don't have to be part of that statistic—welcome to the Duck Side!

Dax the duck

We're the Internet privacy company for everyone who's had enough of hidden online tracking and wants to take back their privacy now.

Read More



DuckDuckGo Privacy Newsletters

Stay protected and informed with our privacy newsletters.

Your email address

SUBSCRIBE

Your email address will not be shared or associated with anonymous searches.

— Spread Privacy —

Crash Course

How to Check Whether Your Web Connection's Secure

How to Set Up Your Devices for Privacy Protection

See all 17 posts →

CRASH COURSE

Are Ads Following You?

Recently we wrote a post about how “private browsing” modes aren’t really private. They still let websites track you across the net. But why all this tracking? Let’s take the prime

1 MIN READ

DUCKDUCKGO NEWS

2017 DuckDuckGo Donations: $400,000 to Raise the Standard of Trust Online

seventh year we are making donations to organizations that share a similar vision. We are lucky

4 MIN READ

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #703

THE PROBLEM SOLVER

By Michael Connell, Computerworld
APR 4, 2017 10:42 AM PDT

OPINION

You are not very incognito in incognito mode

If you are concerned about your online privacy, you should know what incognito mode does and doesn't do to protect it.

Modern browsers offer an increased privacy option that goes by a number of different names: Incognito Mode in Chrome, Private Browsing in Firefox and Opera, InPrivate Browsing in Internet Explorer and Microsoft Edge, and Private Window in Safari. Since all of these do more or less the same thing, so I'll just use Chrome's "Incognito Mode" moniker as shorthand to refer to all of them.

When you open an incognito window in Chrome, the most popular browser choice, there is a description that explains the limits of what is protected from prying eyes. Judging from a number of conversations I've had, this description is often ignored. A surprisingly high percentage of people mistakenly think that going incognito hides their activity from all prying eyes. As Google's description of incognito mode makes clear, this is not the case:

"Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

[Related: Online privacy: Best browsers, settings, and tips]

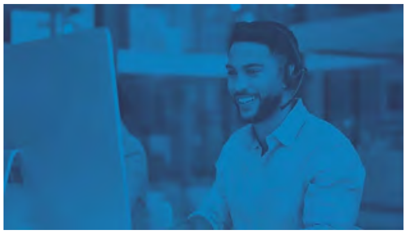
However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit."

There are two types of privacy to consider: local privacy and online privacy. Only your local privacy, what people can see on the computer where your browsing takes place, is effected by switching to incognito mode. Your online privacy is not impacted in any way.

Basically, incognito mode just means that the browser doesn't save cookies, temporary internet files or your browsing history when you are in incognito mode. The main thing it does is hide your browsing history from other people who use the same computer. Not all of reasons someone might want to do this are nefarious; I used incognito mode when I was shopping for Christmas presents on a shared computer this past year, and successfully managed to keep the gifts I searched for and purchased a secret.

There are other uses for incognito mode apart from keeping your browsing history secure from prying eyes. For example, you can be logged into your main Google account, then open an Incognito Window and use it log into a separate or secondary Google account at the same time. The same is true for other accounts that you might not want tracking your every online move, such as Facebook.

Many users have a mistaken understanding about the limits of what incognito mode can do. Despite the clear warnings offered when opening an incognito tab, some still think that it hides their online activity from everyone, including their ISP or employer, when this is obviously not the case. Perhaps it is the "spy in a fedora" icon that Google uses for incognito mode leads some to this mistaken conclusion, but it does absolutely nothing to keep your ISP or employer from seeing exactly what you are doing online, and this mistake could potentially lead to some embarrassing conversations at the office.



In addition, software that is installed on your computer can also circumvent the privacy protections of going incognito. Parental monitoring software is generally unaffected by incognito mode, for example. Spyware that is installed on a computer may also continue to collect information despite the use of incognito mode.

Incognito mode and other private browsing modes are useful and they do provide a real level of local privacy protection that is easy to take advantage of. As long as users are aware of the limitations and do not expect a magic bullet that completely hides their online activity, it can be a useful tool that is simple to use.

But if you want real online privacy, you are going to have take some extra steps.

Michael Connell a freelance writer who has focused on solving problems for many years, formerly as a trial lawyer and currently by offering solutions to the everyday problems encountered while using current technology. Michael worked as a freelance editor and moderator for both ITworld Answers and IDG Answers.

Follow

It’s time to break the ChatGPT habit

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #704

How-To Geek Log in

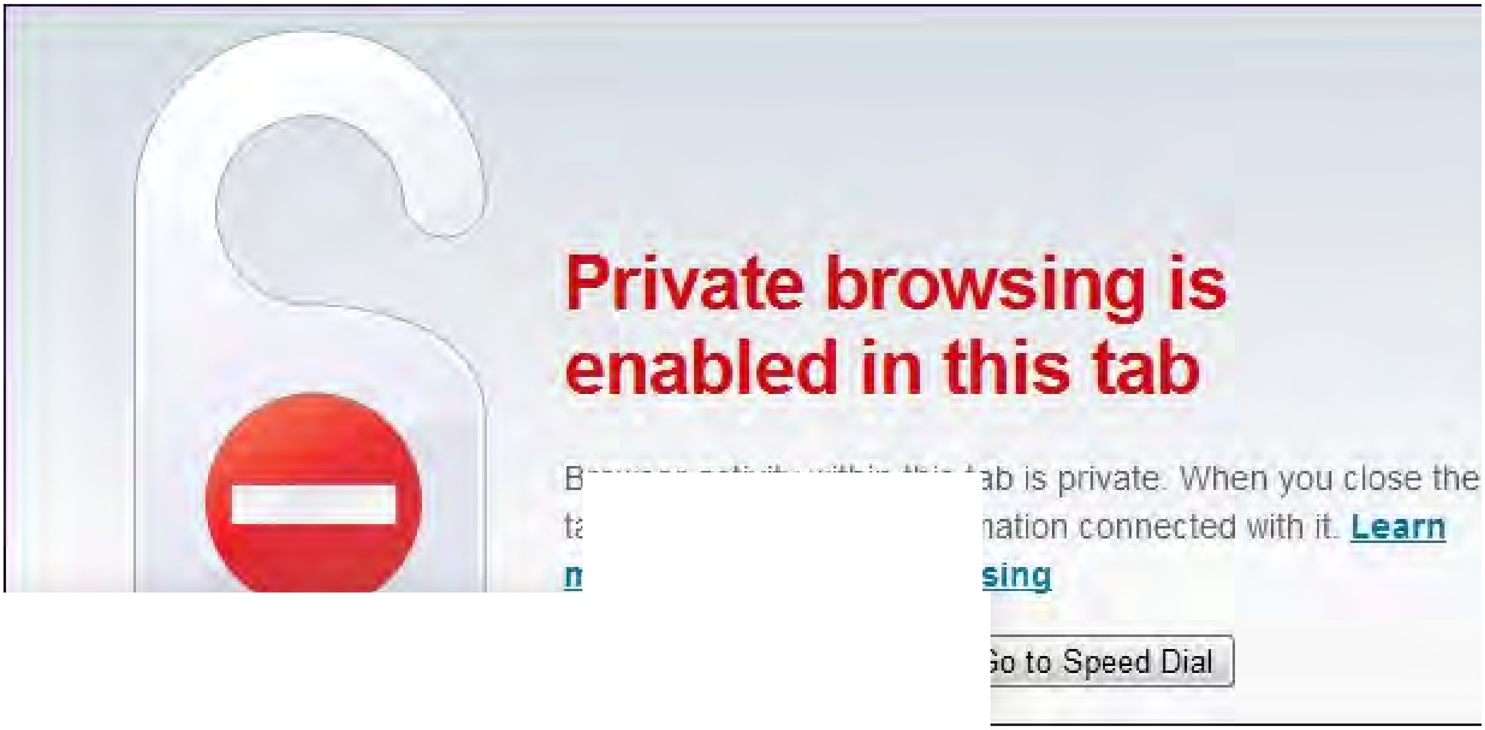
Home › Features

INTUIT mailchimp
The #1 Email Marketing & Automation Platform
Get Started
Based on self-reported worldwide numbers of customers 2021/2022

How Private Browsing Works, and Why It Doesn't Offer Complete Privacy

Private Browsing, InPrivate Browsing, Incognito Mode – it has a lot of names, but it's the same basic feature in every browser.

BY CHRIS HOFFMAN PUBLISHED AUG 29, 2016



Private browsing is enabled in this tab

B ab is private. When you close the

ta nation connected with it. Learn

n sing

Go to Speed Dial

Quick Links

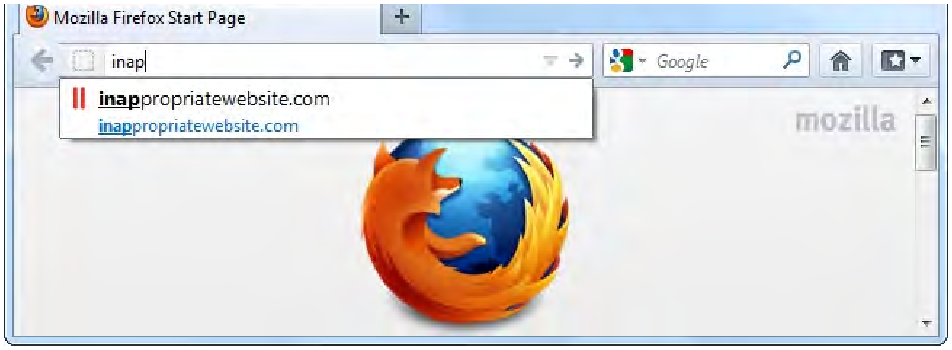
Private Browsing, InPrivate Browsing, Incognito Mode – it has a lot of names, but it's the same basic feature in every browser. Private browsing offers some improved privacy, but it's not a silver bullet that makes you completely anonymous online.

Private Browsing mode changes the way your browser behaves, whether you're using Mozilla Firefox, Google Chrome, Internet Explorer, Apple Safari, Opera or any other browser – but it doesn't change the way anything else behaves.

What Browsers Normally Do

When you browse normally, your web browser stores data about your browsing history. When you visit a website, your browser logs that visit in your browser history, saves cookies from the website, and stores form data it can autocomplete later. It also saves other information, such as a history of files you've downloaded, passwords you've chosen to save, searches you've entered in your browser's address bar, and bits of web pages to speed page load times in the future (also known as the cache).

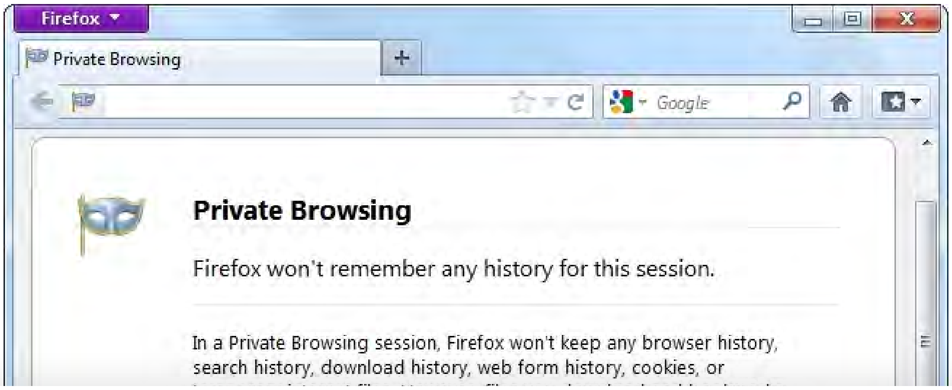
Someone with access to your computer and browser could stumble across this information later – perhaps by typing something into your address bar and your web browser suggesting a website you've visited. Of course, they could also open your browsing history and view the lists of pages you've visited.



What Private Browsing Does

When you enable Private Browsing mode – also known as Incognito Mode in Google Chrome and InPrivate Browsing in Internet Explorer – your web browser doesn't store this information at all. When you visit a website in private-browsing mode, your browser won't store any history, cookies, form data – or anything else. Some data, like cookies, may be kept for the duration of the private browsing session and immediately discarded when you close your browser.

When private-browsing mode was first introduced, websites could get around this limitation by storing cookies using the Adobe Flash browser plug-in, but Flash now supports private browsing and won't store data when private-browsing mode is enabled.



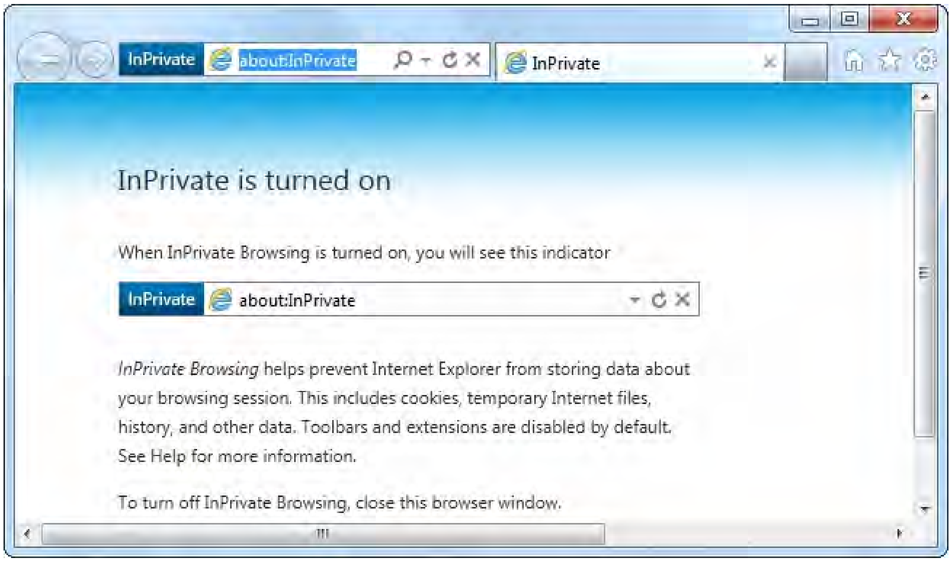
Private Browsing

Firefox won't remember any history for this session.

In a Private Browsing session, Firefox won't keep any browser history, search history, download history, web form history, cookies, or

Private browsing also functions as a completely isolated browser session – for example, if you're logged into Facebook in your normal browsing session and open a private-browsing window, you won't be logged into Facebook in that private-browsing window. You can view sites with Facebook integration in the private-browsing window without Facebook tying the visit to your logged-in profile. This also allows you to use the private-browsing session to log into multiple accounts at once – for example, you could be logged into a Google account in your normal browsing session and log into another Google account in the private-browsing window.

Private browsing protects you from people with access to your computer snooping at your browsing history – your browser won't leave any tracks on your computer. It also prevents websites from using cookies stored on your computer to track your visits. However, your browsing is not completely private and anonymous when using private-browsing mode.



InPrivate is turned on

When InPrivate Browsing is turned on, you will see this indicator

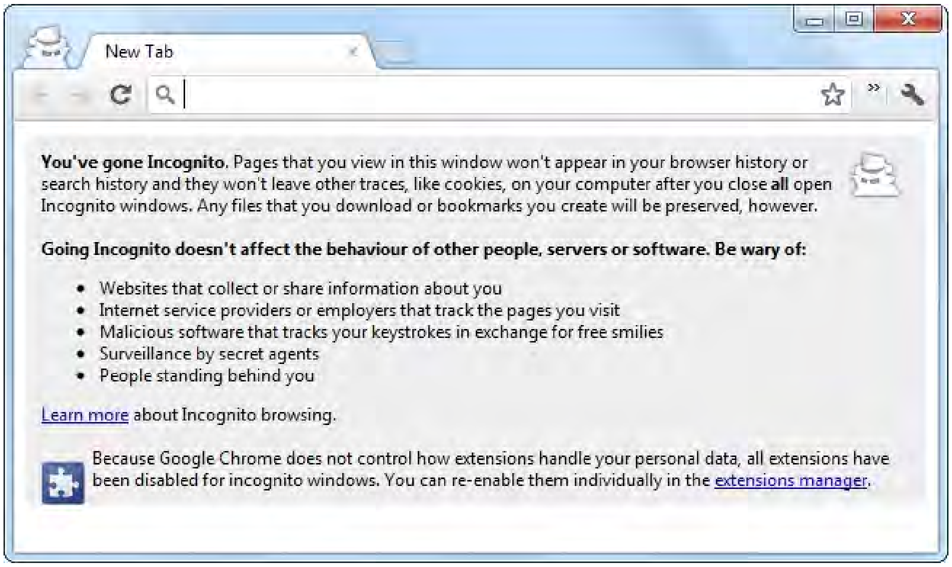
InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.

To turn off InPrivate Browsing, close this browser window.

Threats On Your Computer

Private Browsing prevents your web browser from storing data about you, but it doesn't stop other

can still snoop while it's occurring – assuming they have access to your computer. If your computer is secure, you shouldn't have to worry about this.



You've gone Incognito. Pages that you view in this window won't appear in your browser history or search history and they won't leave other traces, like cookies, on your computer after you close **all** open Incognito windows. Any files that you download or bookmarks you create will be preserved, however.

Going Incognito doesn't affect the behaviour of other people, servers or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smilies
- Surveillance by secret agents
- People standing behind you

Learn more about Incognito browsing.

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can re-enable them individually in the extensions manager.

Network Monitoring

Private browsing only affects your computer. Your web browser can decide not to store browsing activity history on your computer, but it can't tell other computers, servers, and routers to forget your browsing history. For example, when you visit a website, the traffic leaves your computer and travels through several other systems to reach the website's server. If you're on a corporate or educational

Private browsing doesn't stop any of this logging. It doesn't leave any history lying around on your computer for people to see, but your history can always be – and usually is -- logged elsewhere.

image

If you really want to browse the web anonymously, try downloading and using Tor.

Chris Hoffman is the former Editor-in-Chief of How-To Geek. Chris has personally written over 2,000 articles that have been read more than one billion times—and that's just here at How-To Geek.…

ANDROID IPHONE

Google Wallet Now Supports Barcode and QR Code Passes

4 hours ago

How to Enable Wi-Fi Calling on Android

1 day ago

What's the Latest Version of Android?

Google's Pixel 8 Has Some Camera Issues

3 days ago

See More

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #705

thrillist

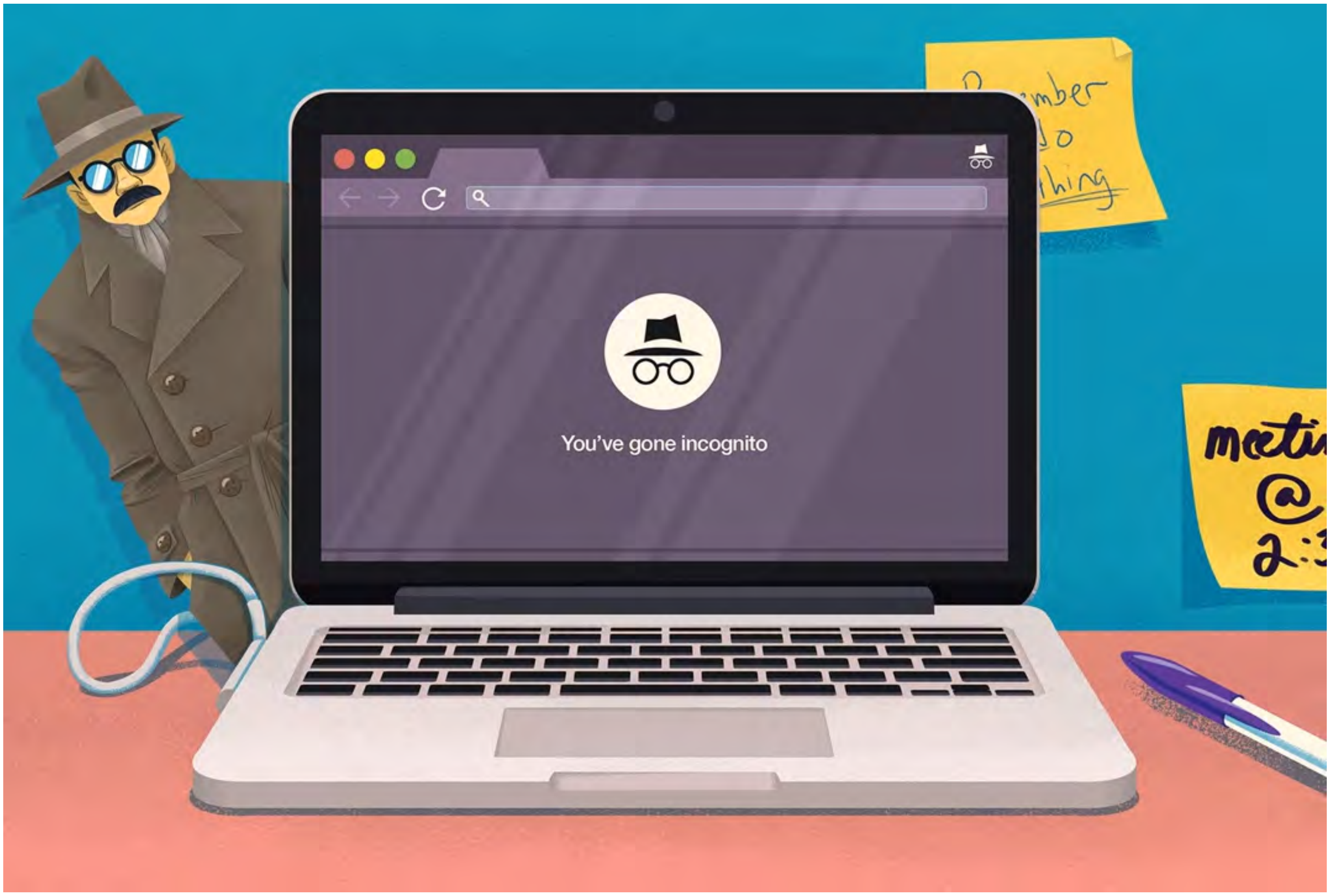
SUBSCRIBE

CITIES + NEWS TRAVEL EAT DRINK

What Chrome's Incognito Mode Is Actually For, Explained By a Google Exec

By Joe McGauley

Published on 11/20/2017 at 12:01 AM



Jason Hoffman/Thrillist

In December 2008, the internet welcomed Google's Incognito Mode, a privacy option for Chrome, with open arms. The feature offered protection against overbearing browser-history snoops at a time when many of us considered getting caught visiting NSFW sites (OK, let's be frank: *porn*) on a computer to be the biggest threat posed by the web. This wasn't exactly the case.

In fact, hiding your unmentionable browsing habits was hardly the reason a crack team of developers at Google made Incognito Mode. Knowing that Incognito Mode is still widely misunderstood, and has somewhat unfairly come to connote shady behavior, we talked to one of the people who built it, Google's Vice President of Chrome, Darin Fisher. Fisher provided a firsthand take on how people should be using it, and what people *shouldn't* be expecting it to do for them.

Incognito Mode will not help you watch porn at work...

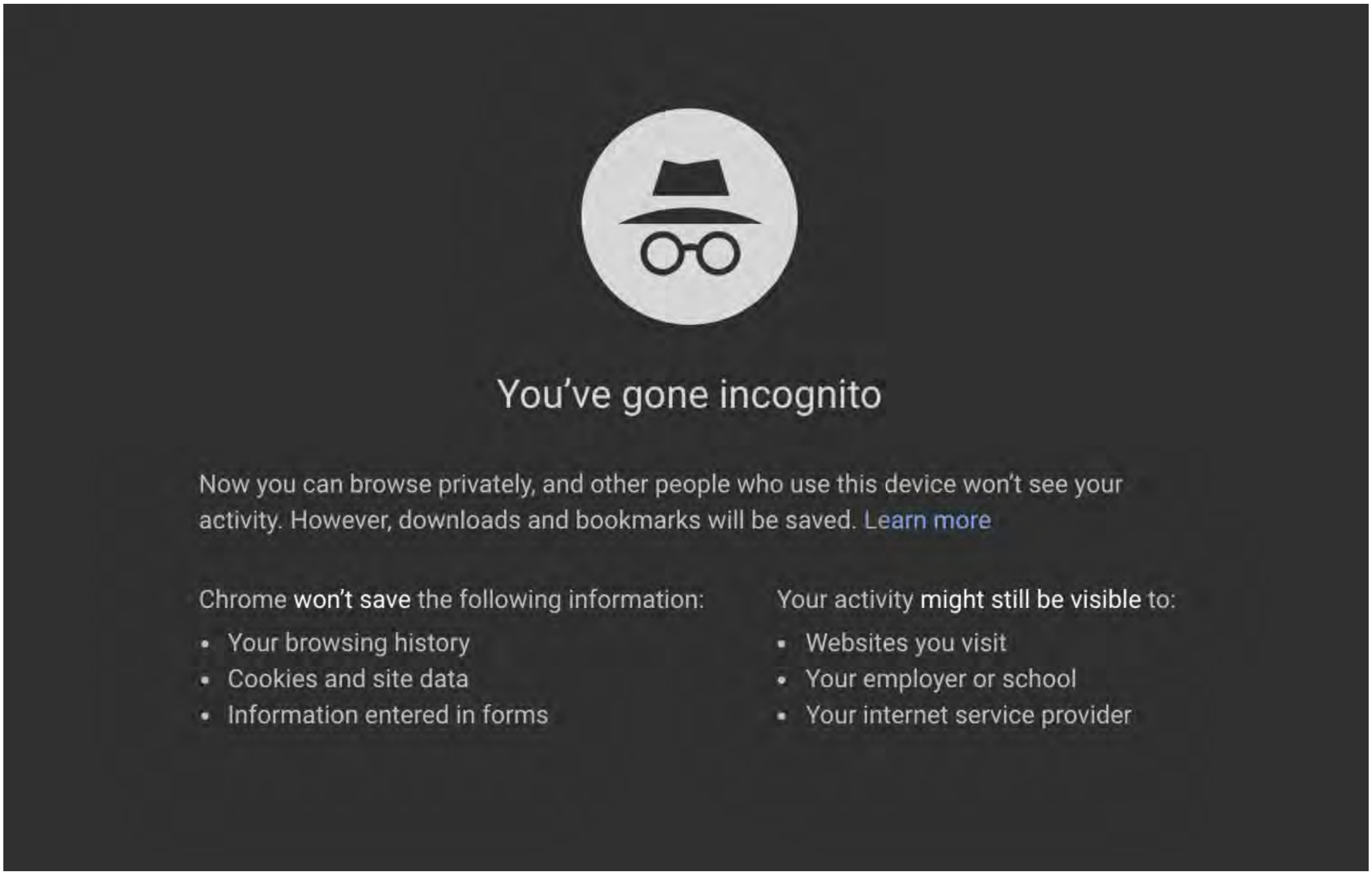
Although Incognito Mode has earned a reputation for helping people shield prying eyes from seeing whatever it is they don't want to be caught having looked at, its origins are far from illicit. According to Fisher, Incognito Mode was born in 2008 with the primary intention of making it easier and more convenient for people who share computers to do so without mucking up their devices with another user's cookies -- the temporary or permanent files stored on your computer by websites to help them recognize you and keep track of your preferences.

That said, it was also meant to help people hide behaviors they didn't want loved ones to see. Though, as Fisher describes it, the scenario Google envisioned involves a boyfriend searching for engagement rings who doesn't want his soon-to-be-fiancée -- with whom he shares a computer -- to get any hint that he's about to propose. The Chrome team wanted to provide a tool that would enable people to "pause" their browser from recording its history so people wouldn't have to purge it in its entirety whenever they didn't want to leave a trace -- a move Fisher describes as "destructive" because it prevents your browser from taking advantage of historical data (e.g., cookies) to power future searches, and causes it to slow down.

... in fact, if you're using it that way, your boss can probably still see what you're doing

When you use Incognito Mode, your browsing activity does not get recorded to the physical device you're using. That doesn't mean all of what you do is necessarily invisible to the people you want to keep in the dark. That's because if you browse an unsecure site (one without an "https") people who are on the same network as you could peek at what you're doing, and see the sites you're seeing.

For example, if you log on to your employer's Wi-Fi using Incognito in hopes of getting away with something shady online, a savvy superior could easily watch as you go about your business. As more and more sites opt to more secure "https" domains this is becoming less of an issue, but the fact remains that Incognito Mode will not protect you from snoops in this scenario.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Google (Screencap)

Incognito Mode was not designed to protect your privacy

If you want to conceal the fact you're about to propose to your partner by doing some covert ring shopping on Incognito Mode, do it! But if you expect IM to protect you against the many, many privacy pitfalls inherent to browsing the modern-day web, be aware that's not its purpose. In fact, Fisher explained that the Chrome team agonized over what to call IM it in the beginning, intentionally steering away from including "privacy" in the name, because it didn't want to oversell its ability.

"When you launch the Incognito tab there’s this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school your, and to your ISP [internet service provide] of course," he says.

What Incognito Mode *is* useful for

While its developers intended Incognito Mode to make sharing your computer easier, it's since become a handy tool in a number of other situations. For instance, some old-hat flight deal searchers claim they've found cheaper fares while doing repeat flight searches in IM, so as to prevent airlines from keeping tabs on their activity and freezing or jacking the price.

It's also a good way to protect yourself against potentially sketchy or unsecure sites you casually encounter. Fisher suggests this is actually one of its best uses, and encourages people to right click on hyperlinks in Chrome and launch them by selecting "Open Link in Incognito Window." Also, consider shopping on Amazon in IM if you don't want the site's pesky "similar item" suggestions to follow you everywhere you go.

The bottom line is, be vigilant and keep your browser updated

While Fisher didn't give us his take on how best to browse without leaving any trace whatsoever, and acknowledges that Incognito Mode should not be considered a privacy shield, he maintains that the best way to protect yourself and your privacy in the age of rampant online identity theft and hacking is to make sure you're using a modern browser and keeping it updated. The Chrome team is constantly monitoring threats and bugs, and ensures its updates include patches and fixes to address whatever security breaches people are most at-risk of, he said.

The truth is, the only way to be truly invisible online these days is to use a browser like Tor on the Dark Web. Then again, if you don't know what that is or how to get there, you should probably steer clear -- "Dark" is the word that describes it in more ways than one.

Sign up here for our daily Thrillist email and subscribe here for our YouTube channel to get your fix of the best in food/drink/fun.

Joe McGauley *is a senior writer for Thrillist. Follow him @jwmcgauley.*

By signing up, I agree to the Terms and Privacy Policy.

Sponsored Content

Related

ENTERTAINMENT SEP 14, 2022

Whitney Is Holding Onto a 'SPARK' of Optimism

ENTERTAINMENT SEP 1, 2022

Never Will Maitreyi Ramakrishnan Forget This Feeling

ENTERTAINMENT AUG 29, 2022

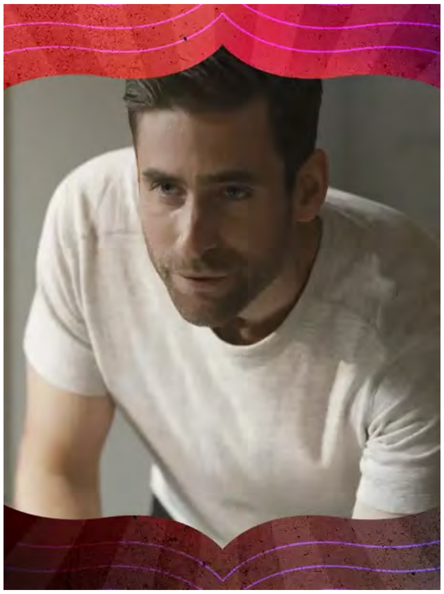
Daryl McCormack Is the Summer's Breakout Star

ENTERTAINMENT AUG 15, 2022

Zoey Deutch Is in Her Dream Come True at Russ & Daughters

ENTERTAINMENT AUG 8, 2022

Why the Shocking Twist in 'Bodies Bodies Bodies' Is so Killer



ENTERTAINMENT AUG 2, 2022

Oliver Jackson-Cohen Likes to Play the Bad Guy

ENTERTAINMENT AUG 1, 2022

On 'Renaissance,' Beyoncé Demands Joy

ENTERTAINMENT AUG 1, 2022

How Lena Dunham and Kristine Froseth Created the Eccentric Heroine of 'Sharp Stick'

ENTERTAINMENT JUL 29, 2022

Rebecca Hall Stares Down Terror in 'Resurrection'

ENTERTAINMENT JUL 29, 2022

How Scammers, TikTokers, and Satires Inspired 'Not Okay'

ENTERTAINMENT JUL 29, 2022

Myha'la Herrold and Ken Leung Are the Captains of 'Industry'

ENTERTAINMENT JUL 29, 2022

Amazon's 'Paper Girls' Is a Promising Adaptation of a Fantastic Comic Series

LOAD MORE

Cookie Settings

Newsletter

Accessibility

Advertise With Us

Careers

Cookie Policy

Do Not Sell or Share My Personal Information

Press

Privacy

Terms + Conditions

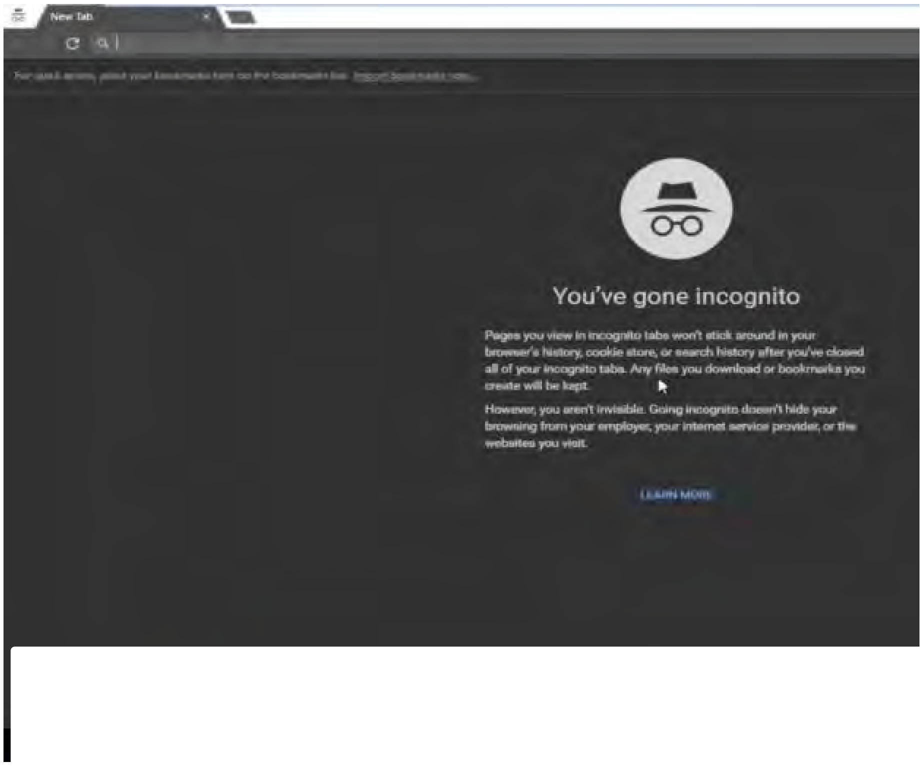
PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #706

Trusted Reviews

Trusted Reviews is supported by its audience. If you purchase through links on our site, we may earn a commission. Learn more.

Explained: What does Googl Incognito Mode actually mea

By Roland Moore-Colyer
November 20, 2017 8:09 pm GMT

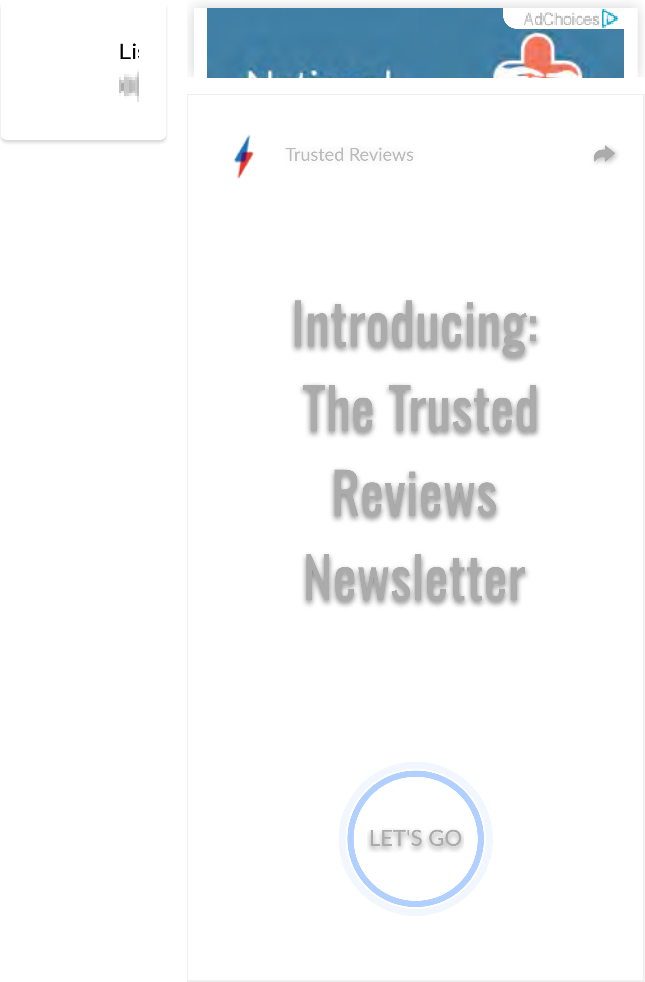

New Tab
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Credit: YouTube



Trusted Reviews

Introducing: The Trusted Reviews Newsletter

LET'S GO

By Roland Moore-Colyer

Why trust our journalism?

Founded in 2003, Trusted Reviews exists to give our readers thorough, unbiased and independent advice on what to buy.

Today, we have millions of users a month from around the world, and assess more than 1,000 products a year.

Editorial independence

Editorial independence means being able to give an unbiased verdict about a product or company, with the avoidance of conflicts of interest. To ensure this is possible, every member of the editorial staff follows a clear code of conduct.

Professional conduct

We also expect our journalists to follow clear ethical standards in their work. Our staff members must strive for honesty and accuracy in everything they do. We follow the IPSO Editors' code of practice to underpin these standards.

Recommended for you

Recommended by Outbrain

Sponsored

Now part of your world

Experience the global phenomenon. Disney's The Little Mermaid is streaming on Disney+.

Disney+

Sponsored

See Search Results For Top New Device For Sleep Apnea

Yahoo! Search

Sponsored

Sponsored

The New Kia Telluride Will Leave You Speechless (See Prices)

PopularSearches | Search Ads

New York Will Cover the Cost to Install Solar if You Live in These Zips

Find out if you qualify. Get your free quote today!

EasySolar

Playboy abandons nudity, blames the internet

TrustedReviews

Microsoft confirms it's retiring the Surface Book…

TrustedReviews

Sony PS5 Slim: Smaller, lighter, with detachable…

TrustedReviews

The iPhone 15 gets a dramatic UK price drop

TrustedReviews

Sponsored

New 2023 Hybrid SUVs - The Prices Might Leave You Speechless

PopularSearches | Search Ads

Sponsored

Early Signs & Symptoms Of Macular Degeneration Seniors Should Look O…

SearchFavorites | Search Ads

Sponsored

See Why Americans Are Switching To Hyundai (The Prices Might Surprise…

PopularSearches | Search Ads

Sponsored

If you're over 42 years old, this realistic game is a must!

RAID: Shadow Legends

PLAINTIFF’S MOTION *IN LIMINE* 2; Google Exhibit #707

Tech

Incognito mode doesn't protect your privacy and can let your boss see what you're browsing

'Your activity isn't hidden from websites you visit, your employer or school, or your internet service provider'

Aatif Sulleyman • Monday 20 November 2017 13:02 GMT • Comments

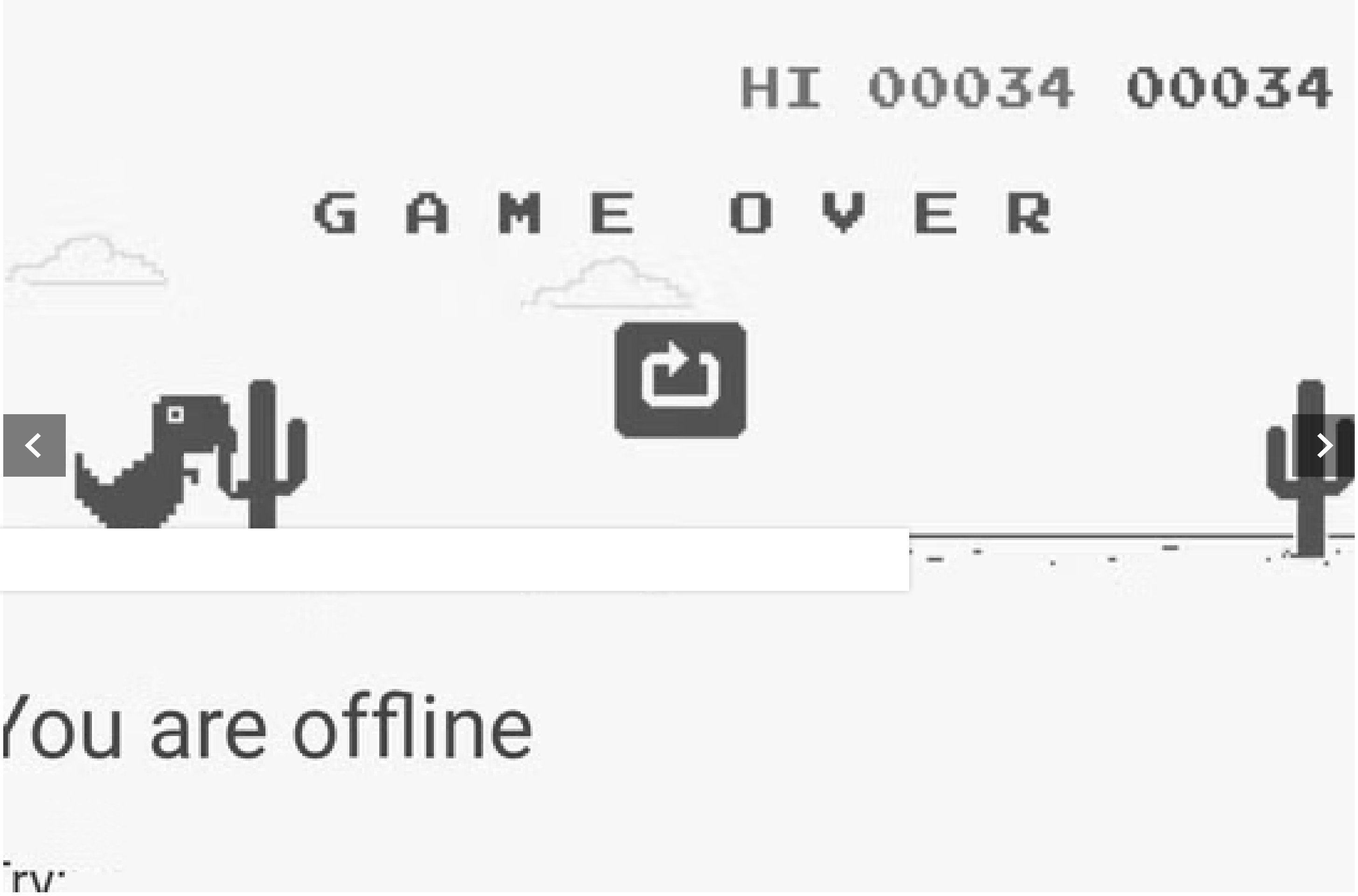
People can still monitor what you do online even when you use Google Chrome's incognito mode, a Chrome developer has explained.

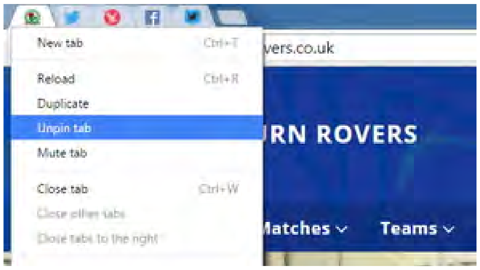
While incognito mode stops Chrome from saving your browsing activities, they could still remain visible to others.

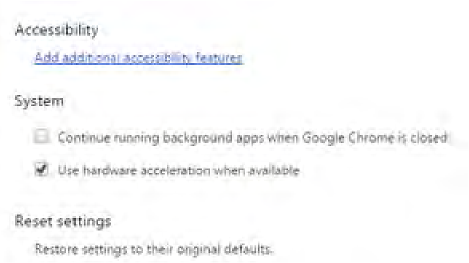
It’s bad news for anyone who uses incognito mode to access NSFW content online.

11 hidden Google Chrome features you didn't know existed

Show all 11






Accessibility

Add additional accessibility features

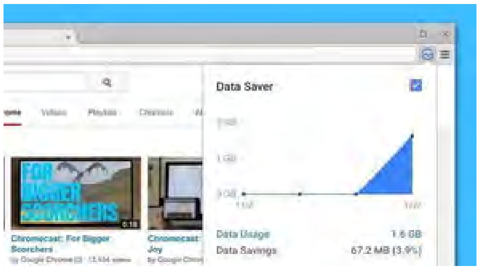
System

□ Continue running background apps when Google Chrome is closed

☑ Use hardware acceleration when available

Reset settings

Restore settings to their original defaults.



According to Chrome developer Darin Fisher, Google "agonised" over what to name the feature, deliberately choosing not to call it “privacy mode” in order to avoid misselling it to users.

“When you launch the incognito tab there’s this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school, and to your [internet service provide] of course,” he told Thrillist.

Indeed, whenever you enter incognito mode or open a new incognito mode tab, a short message appears on-screen, briefly explaining how it works.

It says Chrome won’t save your browsing history, cookies and site data, and information entered in forms, when you’re in incognito mode.

However, Google adds that your activity “might still be visible to” websites you visit, “including the ads and resources used on those sites”; your employer, school, or whoever runs the network you’re using; and your internet service provider.

RECOMMENDED

› Phone companies ranked for connections to wars, human rights abuses

Google reiterates this on its incognito mode help pages, saying, “Your activity isn’t hidden from websites you visit, your employer or school, or your internet service provider.”

Amongst other things, that means your boss could figure out if you’re doing something you’re not supposed to at work, even if you’re browsing incognito.

Mr Fisher instead recommends using incognito mode for avoiding cookies, hiding activities from people who may have access to your computer, such as a loved one you're buying a present for, and protecting yourself against potentially dodgy websites.

More about: Google Google Chrome Privacy

Join our commenting forum

Join thought-provoking conversations, follow other Independent readers and see their replies

Comments

NEWS

Steve Bell 'sacked' by Guardian in antisemitism row over Netanyahu cartoon

NEWS

Symptoms of new Covid variants as cases increase

LIFESTYLE

Richard E Grant says there are friends he 'won't speak to again' after wife's death

CULTURE

Beverley Knight makes Strictly clarification after false accusation from viewers

‘I’d get less hassle for murder’: Man accused of felling Sycamore Gap tree speaks out

GET IN TOUCH

Contact us

OUR PRODUCTS

Subscribe

Register

Newsletters

Donate

Today’s Edition

Install our app

Archive

OTHER PUBLICATIONS

International editions

Independent en Español

Independent Arabia

Independent Turkish

Independent Persian

Independent Urdu

Evening Standard

LEGAL

Code of conduct and complaints

Contributors

Cookie policy

Donations Terms & Conditions

Privacy notice

User policies

Modern Slavery Act

EXTRAS

Advisor

Puzzles

All topics

Betting

Voucher codes

Compare

Competitions and offers

Independent Advertising

Syndication

Working at The Independent

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #708

HUFFPOST

This article exists as part of the online archive for HuffPost Australia, which closed in 2021.

TECH ALPHABET INC COMPUTER SOFTWARE AND APPLICATIONS GOOGLE

Google Chrome's Incognito Mode Isn't That Incognito

Yes your boss can probably still see your browsing history.

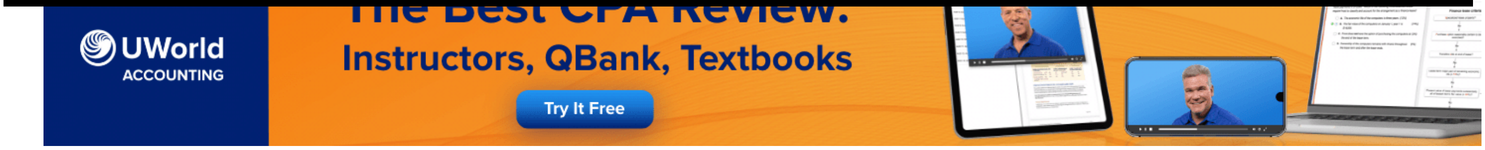
By Thomas Tamblyn

Nov 21, 2017, 03:17 PM EST

A developer for Google's Chrome browser has finally confirmed some bad news, Incognito Mode on Chrome isn't actually that Incognito.

In fact most browsers who offer a 'private browsing' mode won't be able to keep the websites you visit hidden from your internet provider or your boss.

GOOGLE



Speaking to Thrillist, software engineer at Google Darin Fisher revealed the realities of Incognito Mode.

Turns out that while Chrome's secretive browsing feature is still very useful, it's absolutely not going to be keeping your employer from seeing what you do, which is in fact why it's only called Incognito Mode and not something more definitive.

Instead what Incognito Mode actually does is 'pause' the recording processes that go on from cookies to browsing history and even searches.

This makes it perfect if you're looking for gift ideas on a shared laptop but not so good if you're trying to mix business with personal at work.

The issue here lies in the what websites secure themselves. If you visit a website that doesn't start with 'https' then it's probably not that secure and your admin is still going to be able to see it.

Related...

- Quiz: What Do You Really Know About Online Privacy?

Study

If it does start with 'https' then you're in better luck, but again this is only going to give you some element of protection. In some countries ISPs are required by law to have some record of your internet usage so while they might not be able to see the messages you sent through that browser, they could see when you logged on and potentially even the website you visited.

For those of you who are keen to exercise your right to privacy then experts have long recommended that you utilise a VPN.

This, combined with a browsing mode like Incognito Mode or Safari's Private Browsing should give you a solid amount of security against wish).

Of course VPNs come with their own downsides which is that if you're thinking of using them to watch Netflix from another country then you're going to be sorely mistaken.

One particularly good side-effect of private browsing modes, and in particular Apple's is that they can prevent advertisers from learning too much about you.

JUSTIN SULLIVAN VIA GETTY IMAGES

In the new version of Safari Apple has given its browser the ability to automatically stop those videos that will automatically start playing the moment you open a browser.

are the reason you always see a product advertised on another site after you considered buying it.

H/T: The Thrillist

Related Coverage

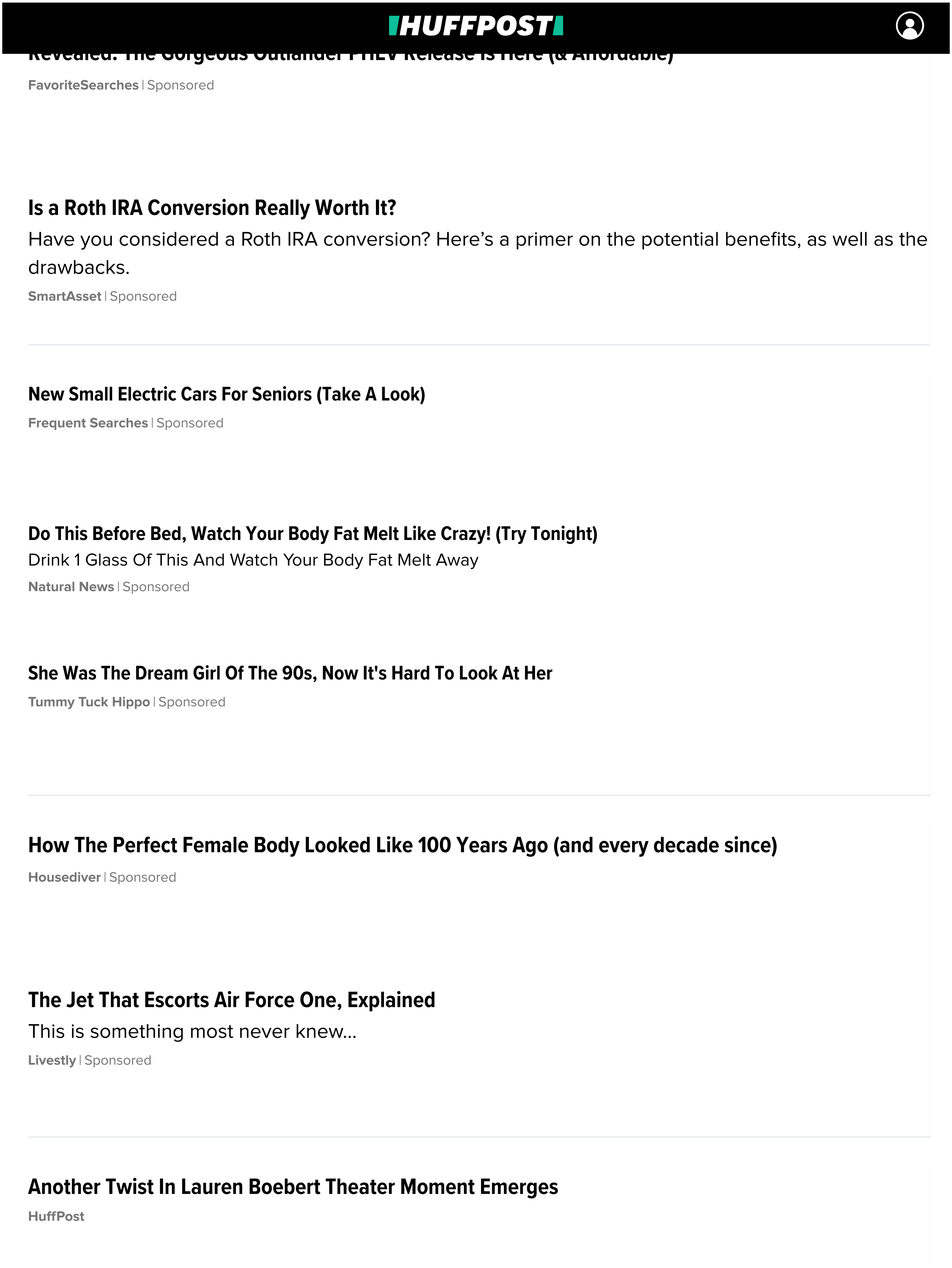
- Google Family Link: How Parents Can Monitor Their Child's Mobile Phone
- Google Maps Now Lets You Zoom All The Way Out To Pluto

Suggest a correction

ALPHABET INC | COMPUTER SOFTWARE AND APPLICATIONS | GOOGLE | GOOGLE CHROME | NETFLIX

Thomas Tamblyn

.



Revealed: The Gorgeous Outlander PHEV Release Is Here (& Affordable)

FavoriteSearches | Sponsored

Is a Roth IRA Conversion Really Worth It?

Have you considered a Roth IRA conversion? Here's a primer on the potential benefits, as well as the drawbacks.

SmartAsset | Sponsored

New Small Electric Cars For Seniors (Take A Look)

Frequent Searches | Sponsored

Do This Before Bed, Watch Your Body Fat Melt Like Crazy! (Try Tonight)

Drink 1 Glass Of This And Watch Your Body Fat Melt Away

Natural News | Sponsored

She Was The Dream Girl Of The 90s, Now It's Hard To Look At Her

Tummy Tuck Hippo | Sponsored

How The Perfect Female Body Looked Like 100 Years Ago (and every decade since)

Housediver | Sponsored

The Jet That Escorts Air Force One, Explained

This is something most never knew...

Livestly | Sponsored

Another Twist In Lauren Boebert Theater Moment Emerges

HuffPost

Ex-Pence Aide Recalls What Trump Said About MAGA Fans In Private: It's Not Good.

HuffPost

This article exists as part of the online archive for HuffPost Australia. Certain site features have been disabled. If you have questions or concerns, please check our FAQ or contact support@huffpost.com.

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #709

What Your Web Browser's Incognito Mode Really Does

This tool can be useful, as long as you understand its limitations

By Nicholas Deleon
June 19, 2018

You don't have to be a computer whiz to grasp the value of private web browsing. At a time when consumers are worried about the data Facebook and others have assembled on their digital lives, it's nice to have a browser tool that conceals some online activity.

All of today's major web browsers–Chrome, Edge, Firefox, and Safari–offer a feature that provides a private browsing window and deletes the browsing history on your computer after you close it. (To open a private window, go to the File menu and look near the New Window option.)

These windows can help reduce the amount of information collected on you by retailers and advertising companies. They have other smart uses, too.

However, recent research (PDF) indicates that many people overestimate the protection provided.

STAY SMARTER ONLINE

More From Consumer Reports

More From Consumer Reports

More From Consumer Reports

The Best Ad Blockers

More than half of 460 people surveyed by University of Chicago researchers thought an incognito window would block Google from recording their search history even if they were logged into their Google account. More than 40 percent of respondents believed the tool would hide their location from websites they visited. And more than one-third believed incognito mode would shield their web browsing from an employer.

None of that is true.

"Private browsing mode does some useful things, but you're absolutely not anonymous, you're not ‘incognito,' and your secrets are not necessarily safe" from hackers or marketers, says Blase Ur, an assistant professor of computer science at the University of Chicago who conducted the research. "You should still browse like people are watching."

Here's what private browsing really does—and what it doesn't do.

How Does Incognito Mode Work?

When you browse the web in a regular, nonincognito window, the browser stores the URL, or web address, of every page you visit and keeps that information even after you close the window you're in. That makes it easier for you to retrace your steps and find the same web pages again sometime later.

The browser also stores cookies, which are little files that websites and advertisers embed in websites. Next time your browser loads a page with elements from a company's servers, the information is sent back. Cookies have lots of functions, such as letting you go to password-protected sites without logging in each time and keeping track of what you place in a shopping cart. They also let big advertising companies, such as Google's DoubleClick, track you from site to site across the web.

Private windows act differently.

If you're using incognito mode, "At the end of each session your cookies go away and you get a whole new set the next time you start," Ur says.

The most obvious change you'll notice after a privacy browsing session is that it doesn't show up under the History tab in your browser. But you may also notice less tracking from advertisers. If you search for a product—blenders, say—in a private window, you're not as likely to start seeing cooking supplies show up in web ads over the next few days.

Firefox adds a layer of tracking protection to its private browsing mode. This helps protect against a technique known as fingerprinting, in which data collectors track you around the web by comparing variables such as which browser version and operating system you're using, which graphics card you have installed, and your IP address.

Why Is Incognito Mode Useful?

"If you just want a brand new session that doesn't remember anything about who you are, then incognito mode will work really well for that," says Jeremy Tillman, product director at Ghostery, one of several browser extensions that block web tracking.

Let's say you're shopping for a gift for your spouse on the family laptop—maybe a day pass for a local spa. Using incognito mode will prevent anyone else who might use that laptop from seeing that you searched the likes of Google and Yelp for "best spas near me." And they won't start seeing spa ads popping up over the following few days.

"Nothing spoils a birthday surprise quite like a targeted ad," says Robert Richter, program manager for privacy and security testing at Consumer Reports.

The same goes if you wanted to watch one quick YouTube video about a celebrity gossip item or World Cup highlights without then being bombarded with related videos the next time you log into the site. An incognito window will keep that from happening.

And, Richter says, incognito mode has "espionage light" uses: If you want to read someone's LinkedIn page without them knowing, you can employ an incognito window.

Incognito mode could also come in handy when you're visiting a friend and want to quickly check your email on his computer without opening his email account. Simply launch an incognito window, sift through your inbox, then close the window.

Consumers who print web-based documents using a public computer at a library or an office supply store may also want to use incognito mode because it will erase any personal data, such as Gmail usernames and passwords, when you close the window.

Don't let incognito mode lull you into a false sense of security, though. Logging into personal accounts from a public computer—or even a friend's—is always a more risky endeavor than your living room. Remember: Guard your passwords, and close that window when you're done.

What Doesn't It Do?

Once you close an incognito window, most of the data about your web session will be deleted, "but only the pieces that were stored on your own computer," Richter says. "The data stored on company servers as a result of your online activity is another story altogether."

A private browsing window can't erase the records of your visit from a website's servers, or from any networks you went through to get to a site. If you're on your employer's WiFi network, your company will know which sites you visited, just as though you weren't using a private window.

If a site isn't safe for work, it's not safe for work in incognito mode, either.

Incognito mode also doesn't do anything to protect you from malware—for that, you should take the usual steps of ensuring that your software is fully updated, that you're running trusted antivirus software from a company such as Avira or Symantec, and that you scrutinize the files you download.

And remember that any bookmarks you make or files you download while in incognito mode will persist after you close the browser.

How Targeted Ads Work

Do you often see online ads that relate to your likes and hobbies? On the "Consumer 101" TV show, Consumer Reports expert Thomas Germain explains to host Jack Rico what targeted ads are and how they work.

Recently Tested Computers

See our full list of computer ratings

HP
Pavilion 31.5

HP
24-cb1217c

HP
Envy TE01-3254

Dell
Inspiron i3910

Dell
Inspiron 3910-5870BLU

Dell
XPS 8950-7518BLK

Dell
XPS 8950-7129BLK

MSI
Pro 22XT 10M484

Apple
Mac Studio

Asus
S500MC-DH704

HP
Pavilion TP01-1214

Dell
XPS Tower

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #710

Does Google Chrome have its own VPN?

VPN By James Laird published April 08, 2019

All you need to know...

Google Chrome
One fast, simple, and secure browser for all your devices
Google Chrome: Fast & Secure
Google LLC
3+
UPDATE
OPEN
4.3
Communication
Similar

Image credit: Google Chrome (Image credit: Shutterstock)

Google Chrome is the world's most popular web browser. But despite its near-ubiquity, many users aren't happy with the way it allows your personal data and online activities to be tracked and, in some cases stored, by advertisers, internet service providers (ISPs) and government agencies. That's why using a Chrome VPN is highly recommended for privacy-conscious users.

It allows you to use the web truly anonymously, leading many to wonder if Google - like rival browser Opera – offers its own service built-in to its browser.

Does Google Chrome have its own VPN? In short, no.

- Discover the very best VPN service
- Are free VPNs safe and can they be trusted?
- Hop straight to our pick of the best Chrome VPN extensions

As with virtually any modern web browser, it does provide a private browsing option, which it calls Incognito Mode. Surfing the web in th means that Chrome won't store your browsing history, cookies, site or remember information entered into online forms.

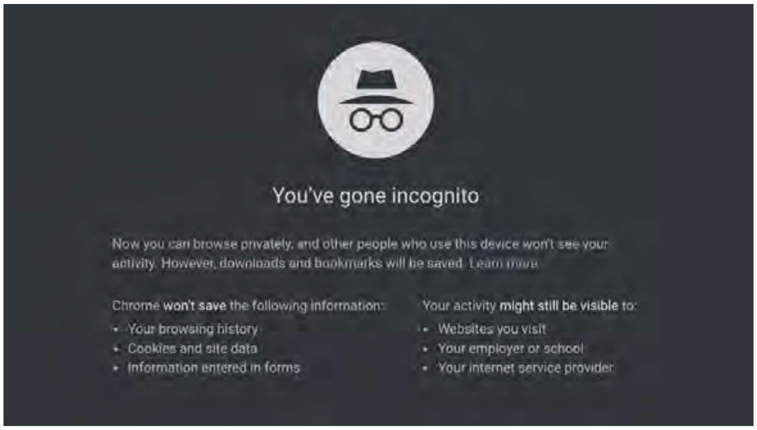
RECOMMENDED VIDEOS FOR YOU...

5 best smartphones of 2023

▶

PLAY SOUND

However, as soon as you enter Chrome's Incognito Mode, it becomes clear it's not the solution truly privacy-conscious users want. Google immediately warns you that using Incognito Mode in Chrome won't hide your activity from the websites you visit, employers and schools or ISPs.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:
- Websites you visit
- Your employer or school
- Your internet service provider

Image credit: Google

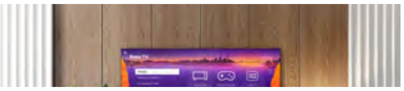
This makes it pretty clear that using Incognito Mode is not the same thing as using a Virtual Private Network in full.

Fortunately, while Google doesn't offer its own service, it does support the use of the dedicated best Chrome VPNs through extensions.

Chrome extensions are essentially little applications that you download to your browser, rather than install to your computer proper. They make it easy to access whatever tool you want to use without having to leave your browser, whether it's a password manager, speller checker, or anything else.

Installing Chrome extensions is a doddle, so while Google's browser might not offer its own VPN, you have a number of options that can installed and activated in a matter of minutes.

MOST POPULAR MOST SHARED



1 Your Roku TV just got a great free update to make it easier to find the movies and shows you love

2 The Samsung Galaxy Ring may launch with the Galaxy Z Fold 6

3 Netflix saves a popular Star Trek animated series as it bizarrely cancels two of its own animated movies

4 The entire Doctor Who collection will be available to stream very soon, but not on Disney Plus

5 Zelda: Tears of the Kingdom director says the Sheikah tech disappeared from the sequel after its "role had been fulfilled"

Our pick of the best extension right now is ExpressVPN, which is affordable (it costs less than $7 a month when buying a year's subscription), easy to use, and crucially, offers a reliable connection.

Finding the best VPN can seem like a daunting task, given how much noise there is surrounding the subject, but after years of testing various services, Express is the one we recommend right now.

A free VPN can seem tempting as well, but they involve making a number of compromises. In some cases, this might be a daily limit on anonymous browsing time and bandwidth, accepting annoying pop-up ads as you browse, or their server network might just be unreliable and prone to cutting out.

That's why coughing up a small amount for a paid option is a better course of action for the truly privacy-conscious web user. It's a brilliant all-round service that packs all the features you need for anonymous web browsing into an easy-to-use package.

As we've already said, it also crucially offers a handy Chrome extension so you can activate and deactivate it at the click of a button whilst browsing. So while Google Chrome might not have its own VPN, there's no need to worry – ExpressVPN is the next best thing. In fact, based on our experience, it might even be better!

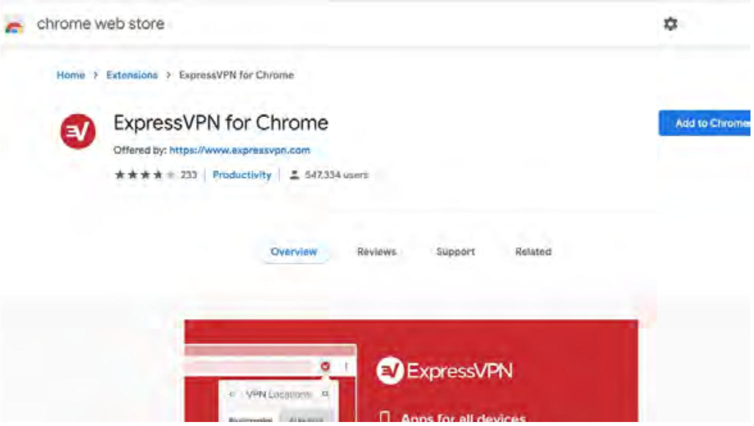


Image credit: ExpressVPN

Should Google Chrome ever introduce its own VPN, we'll update this guide as soon as we get the news. In the meantime, read our full ExpressVPN review to learn more – then check out our guide to enabling a VPN in Chrome to learn how to set yourself up today.

- **Read more:** our guide to the best free VPN
- **Read more:** our guide to the best browsers

TechRadar Newsletter

Sign up to receive daily breaking news, reviews, opinion, analysis, deals and more from the world of tech.

Your Email Address

SIGN ME UP

□ Contact me with news and offers from other Future brands

□ Receive email from us on behalf of our trusted partners or sponsors

By submitting your information you agree to the Terms & Conditions and Privacy Policy and are aged 16 or over.

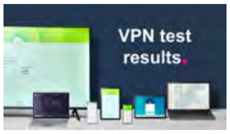
James Laird

James is a technology journalist with nearly 10 years experience and currently Sports and TV Streaming Editor at Future, where he works across TechRadar, T3 and Tom's Guide. He is here to help you find the best ways to watch sports, TV shows and movies online. Previously, he was News and Features Editor at Trusted Reviews, Editor of Lifehacker UK, and Senior Staff Writer at ITProPortal.

MORE ABOUT VPN

LATEST

Private Internet Access' VPN network gets even bigger ▶



Our latest VPN tests are over and the rankings have changed ▶

Look it up, Bookworm - the Raspberry Pi 5 just got its first OS(es) ▶

SEE MORE LATEST ▶

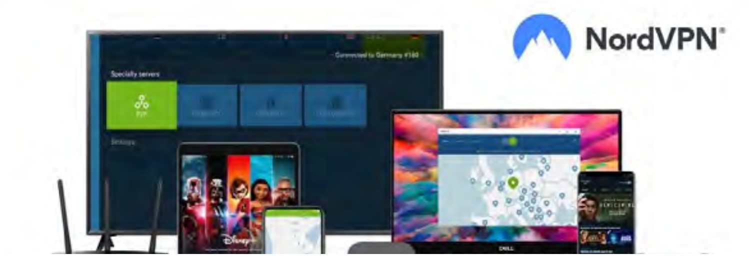
The best free VPN of 2023

We help you pick the best free VPN service in 2023, explaining the pros, cons, and risks. Avoid VPN scams and get a free VPN for streaming Netflix.

MOST POPULAR

Five ways hackers can steal your data on public Wi-Fi

By Nate Drake June 21, 2023



What is NordLynx?

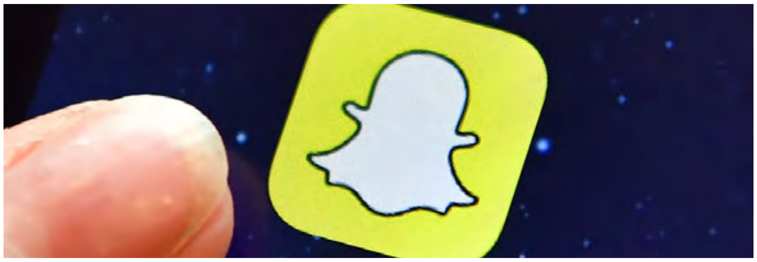
By Nate Drake June 16, 2023

Google Bard VPN: How to access the AI chatbot from anywhere

By Chiara Castro May 26, 2023

Mozilla.ai: not another chatbot

By Chiara Castro May 24, 2023



How to delete your Snapchat account

By Chiara Castro May 03, 2023

Tourist cyber traps revealed: where and why to use a travel VPN

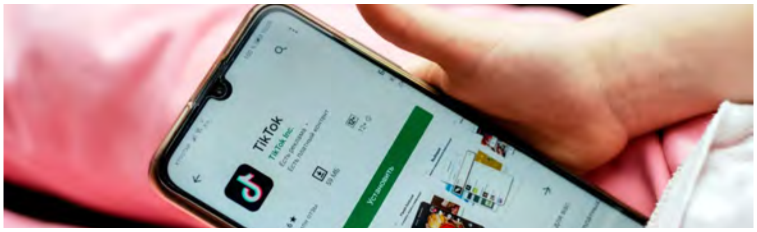
By Chiara Castro April 21, 2023

The best Oman VPN in 2023

By Chiara Castro April 20, 2023

The best Ukraine VPN in 2023

By Chiara Castro March 23, 2023



How to download the TikTok app and bypass bans with a VPN

By Chiara Castro March 21, 2023

Does a VPN slow down your internet? 5 ways to speed up your VPN

By Nate Drake March 16, 2023

Why use a VPN?

By Nate Drake March 10, 2023

TechRadar is part of Future US Inc, an international media group and leading digital publisher. **Visit our corporate site**.

About Us

Contact Future's experts

Contact Us

Terms and conditions

Privacy policy

Cookies policy

Advertise with us

Web notifications

Accessibility Statement

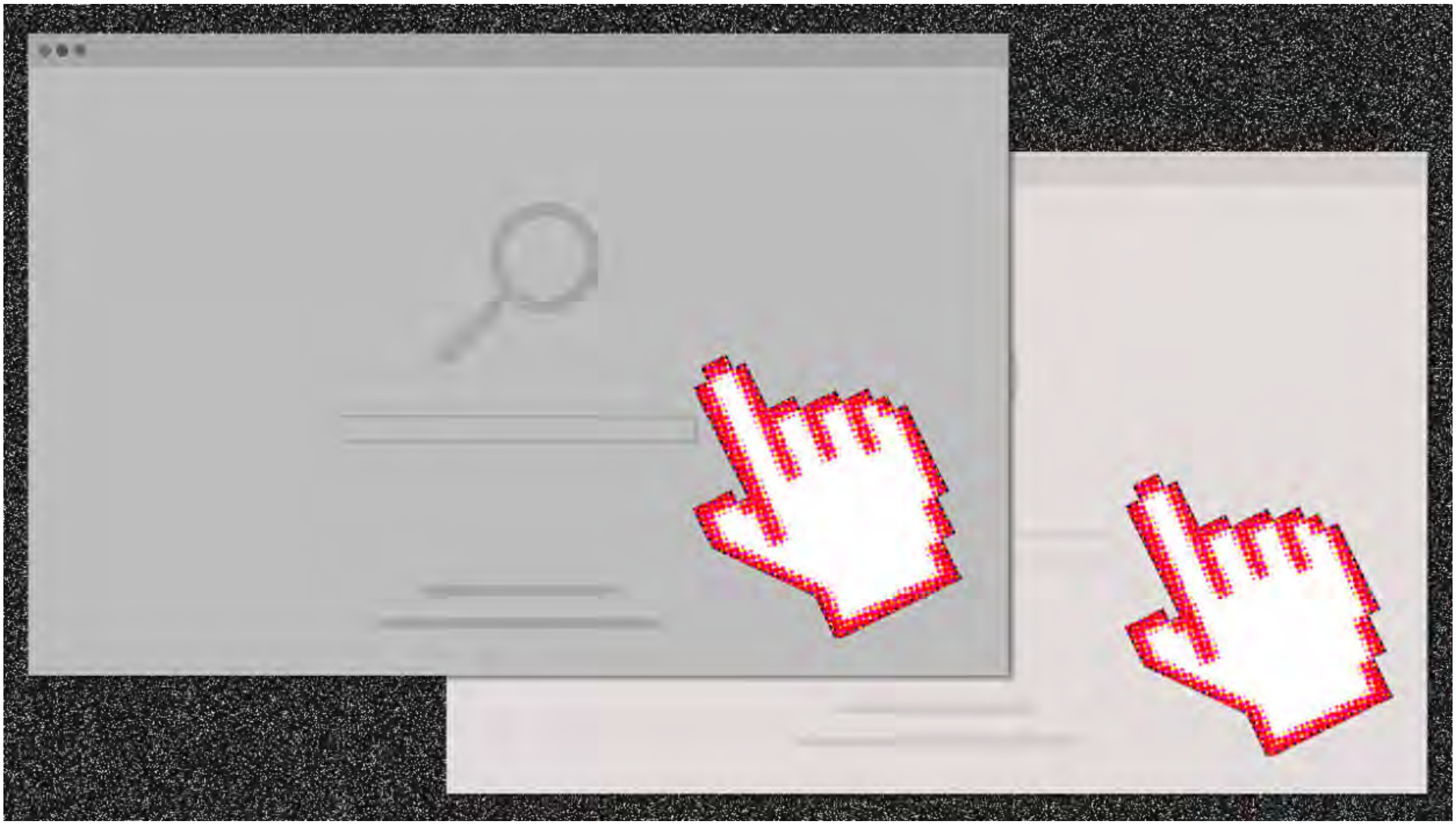
Careers

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #711

04-12-19

Incognito mode won't keep your browsing private. Do this instead

Browser compartmentalization can help you escape the clutches of the data gathering machine.



[Illustrations: janjf93/Pixabay]

This story is part of The Privacy Divide, a series that explores the misconceptions, disparities, and paradoxes that have developed around our privacy and its broader impacts on society. Read the series here.

The big tech giants, online advertising companies, and data brokers use a ton of tricks to track you around the web. These include things like cookies, location and device logging, fingerprinting, and even share buttons, the last of which make it very easy for companies like Facebook and Google to see what you do online, even on third-party websites.

Of course, today's users aren't blind to much of this tracking. And most people who are aware of it will take (somewhat predictable) steps to do what they think will hide their online activity from tech companies.

One of the most common techniques people think can help hide their activity is the use of an "incognito" mode in a browser. This opens a secure browsing window where third-party cookies are blocked and browsing history is paused.

SORRY, NO

The problem with incognito modes is they provide a false sense of security.

Despite what most people assume, incognito modes are primarily built to block traces of your online activity being left on your computer–not the web. Just because you are using incognito mode, that doesn't mean your ISP and sites like Google, Facebook, and Amazon can't track your activity.

This is especially true if you log into any of these sites in your browser after you're in an incognito window–the companies can still see everything you do. And it's the same for any other site you need to log in to. So remember that if you're logged in to a website, no matter if you are using incognito mode, or even a VPN, the website's owners can see exactly what you are doing.

For the people who recognize the limits of incognito mode, they'll generally then use browser extensions to help block more information being sent back to tech companies. These usually involve script, cookie, and ad blockers. The problem with this is that many websites rely on those same technologies to work right–again, this is especially true of websites you need to log into, like banks, social media sites, and shopping sites.

Usually, the sites that require scripts and cookies to work will show you a notification telling you that you need to whitelist them if you want to use the site properly. Whitelisting them gives you back the site's functionality, but then you lose the privacy protections you were seeking in the first place, because those sites will once again place tracking cookies on your computer to follow your online footsteps. So what is a privacy-conscious person supposed to do?

switching between browsers at random, users of browser compartmentalization dedicate one browser to one type of internet activity, and another browser to another type of internet activity.

Here's how it works:

Users will use one browser for any and all websites they need to log in to. This browser is the one on which they'll access their social media, banks, and shopping sites.

The big catch here is that users will never use this browser to search the web or randomly browse the internet. This browser is only used for bookmarked sites you need to log in to. Let's call this your "accounts" browser.

Users will then use a second browser for all their web searching and random browsing. On this browser, a user will never log into any website–ever. They will never use this browser to personally identify themselves in any way, period. We'll call this your "everyday" browser.

By splitting up your web activity between two browsers, you'll obtain the utmost privacy and anonymity possible without sacrificing convenience or the ease of use of the websites you need to log in to. That's because the majority of your web usage will be done in your "everyday" browser, which, by never logging into any website, will make it extremely hard for data firms to identify you and track your activities–especially if you fit your "everyday" browser out with some hardcore privacy extensions. You can go all out with your privacy settings on your "everyday browser": Block all cookies, scripts, and trackers, and always use in it incognito mode. That's because you won't be logging into any sites that require cookies or scripts to be enabled to work.

Related: How the tragic death of Do Not Track ruined the web for everyone

A word of warning: This approach won't completely protect your privacy. Your ISP and other companies may still be able to see which sites you are visiting. To completely obscure your traffic, you'll need to also use a VPN.

For websites that do require those technologies to work, like social media sites and banking sites, you'll use your "accounts" browser.

bookmarks. Thus, when Google or Facebook places a cookie tracker on your “accounts” browser when you log in to their sites so they can track you around the web, this cookie they’ve put on your computer is only accessible through that browser, not any other browser on your computer.

SETTING UP YOUR “ACCOUNTS” BROWSER

When configuring your browser compartmentalization setup on your computer, you’ll want to decide which browser you’ll use as your “accounts” browser, and which one you’ll use for your “everyday” browser. Since your “everyday” browser will be the one you use most often to browse the web, I recommend you use a privacy-focused browser that supports a ton of extensions and add-ons, like Firefox or Brave.

For your “accounts” browser, I still recommend you use a privacy-focused browser, but one that doesn’t require a lot of add-ons or extensions. Remember, you’re going to want to have your “accounts” browser set up to accept some cookies and scripts so you can log in to the websites you need.

That’s why on a Mac I recommend using Apple’s Safari as your “accounts” browser. It’s got decent privacy protections built in, yet ones that won’t break websites you need to log in to. As for a PC, good “accounts” browser options include Microsoft’s Edge, Firefox, and Brave (the latter two are also good options on the Mac). As for Chrome: It’s made by Google, whose sole aim is to know everything you do online, so it’s probably best to stay away from Chrome if you value your privacy.

Once you’ve chosen your “accounts” browser, bookmark every site you use that you log in to: Google, Facebook, your bank accounts, Netflix, airline accounts, utility accounts, Amazon, dating sites, etc. Bookmark them (the toolbar is best for easy access) and access those sites only by clicking on your bookmarks.

Remember: Do not do web searches in this browser. That’s what your “everyday” browser is for. By not searching in this browser nor using it to browse the web, you’ll greatly limit the online activity the websites you do need to log in to can see. But just in case you forget this and do accidentally perform a search, make sure you change the default search engine in your “accounts” browser to DuckDuckGo, the privacy-focused search engine that doesn’t track you.

After you’ve done this, congratulations, your “accounts” browser is now set up.

SETTING UP YOUR “EVERYDAY” BROWSER

The next step is to set up your “everyday” browser. Remember, this is the browser you will use to search and browse the web, so it’s the one you’ll be using most of the time. There are plenty of great browsers to use as your “everyday” browser, but I recommend Firefox because it offers so many built-in security and privacy protections, and even more through extensions. This makes it one of the most secure browsers you can use if set up properly. Other viable options include browsers like Brave and the Tor browser

In your “everyday” Firefox browser, set your content blocking settings to “strict.”

Once you’ve downloaded Firefox, you will want to do the following:

1) Do not bookmark any sites you need to log in to, and never log in to those sites on this browser. Remember that you have your “accounts” browser for that.

2) Go into Firefox’s preferences (Firefox > Preferences) and in the General tab click “Make Default” to make Firefox your default browser. By doing this,

3) Still in Firefox's preferences, click on "Privacy and Security." Under "Content Blocking" choose "strict." This will block known trackers and all third-party cookies.

4) Under "History," check the box labeled, "Always use private browsing mode." This is Firefox's version of incognito mode. Enabling this will ensure your web history is never saved (and thus can never be accessed by a website you visit).

5) Next, you'll want to download three extensions. The first is uBlock Origin. This extension will block the most intrusive ad trackers and malware.

6) Now, install the HTTPS Everywhere extension. This extension is made by the Electronic Frontier Foundation, and it forces your browser to request and use the encrypted version of websites, which mean it's harder for your ISP to track what you do on those sites.

7) Finally, download the Cookie AutoDelete extension. This will automatically delete any cookies, first-party or third-party, that were downloaded during your last browsing session. This ensures that each time you begin a browsing session, no cookies from the last session remain, which makes it almost impossible for sites to track you between browsing sessions.

Once you've done this, your "everyday" browser is now set up. From here on out, all you need to do is remember to keep your online activity compartmentalized between these two browsers. If you need to log in to a site, it's your "accounts" browser you want to go to. If you just want to search or browse the web in relative privacy, simply launch your "everyday" browser.

Remember that browser compartmentalization isn't a perfect privacy method. However, by using browser compartmentalization, you'll make it much harder for the biggest tech companies and data brokers to identify your online activities and track you around the web.

PLUGGED IN

Sign up for our weekly tech digest.

Privacy Policy

ABOUT THE AUTHOR

Michael Grothaus is a novelist and author. His new novel, the speculative fiction 'BEAUTIFUL SHINING PEOPLE', is out now More

LOGIN SUBSCRIBE

CO.DESIGN TECH WORK LIFE NEWS IMPACT PODCASTS VIDEO IF360 FASTC

TECH

TECH

Fake airline reps are helping disgruntled passengers rebook flights in the latest bizarre X scam

TECH

Does the success of 'Naked Attraction' vindicate David Zaslav's strategy for Max?

TECH

Some of the biggest moments of the Sam

NEWS

NEWS

Solar eclipse path 2023: This map shows where to see the 'ring of fire' across the United States

NEWS

These foods and snacks will be impacted by California's ban on harmful additives

NEWS

Gen Z workers expect to retire at age 61, and they aren't afraid to

CO.DESIGN

CO.DESIGN

These morning-after pill ads spin the need for emergency contraception into comedy gold

CO.DESIGN

Spain is building a city from scratch. Can it avoid the mistakes of Saudi Arabia's line-shaped metropolis?

CO.DESIGN

Will Netflix Houses be the

WORK LIFE

WORK LIFE

A better way to buy a home

WORK LIFE

POV: Why you shouldn't include your degree in your signature

WORK LIFE

Forget the crisis. The 'midlife collision' is real and affecting a large part of the workforce

LOGIN SUBSCRIBE

CO.DESIGN TECH WORK LIFE NEWS IMPACT PODCASTS VIDEO IF360 FASTC

Advertise Careers Privacy Policy

Terms Do Not Sell My Data Notice of Collection

Permissions Help Center About Us Site Map

PLAINTIFF’S MOTION *IN LIMINE* 2;
Google Exhibit #712

Science & Tech Latest

Google Chrome Incognito Mode isn’t as private as you think it is, here’s what you should be doing

Andy Gregory

Apr 13, 2019

○ Vote

/ Paula Bronstein/Getty Images/Google Chrome

With recent revelations about the ways in which big-tech uses our browsing data, many have taken steps to shore up their online privacy.

After growing distrust in the way that certain websites and companies use our online data lots of people have turned towards using Google Chrome's 'incognito' browsing in recent years in order to take back control.

The problem? It doesn't do the job many of us assume it does.

Incognito Mode only hides traces of your activity online from those using your computer, not the internet.

It blocks third-party cookies and pauses your internet history, but this has little effect on your ISP and whichever sites you visit being able to follow your activity.

Recommended

What's the Appalachian Trail? The iconic path in today's Google Doodle

People are just learning Google's original name

Google bans Andrew Tate's 'The Real World' App

This problem intensifies further when you log into a website, even if you do so before or after opening an Incognito window. The companies can still track wherever you visit on the internet.

So what can you do to make it harder for companies to see what you do online?

Browser compartmentalisation is a technique that's gained widespread attention recently, for all the right reasons.

Generally speaking, what happens on one internet browser stays on that internet browser.

So, for this privacy technique, you can download multiple browsers, like Chrome, Firefox and Internet Explorer, and separate your activity online.

First of all, decide which browser you want to use for every site you need to log in to, for example social media or financial accounts.

Secondly, choose a different browser on which you'll do all of your internet searches and browsing - activities that will never see you log in to an account.

So now you have your "accounts" browser and your "everyday" browser, which should make it very tricky for big-tech companies to track what you visit.

For those who want absolute peace of mind, consider using a Virtual Private Network (VPN), if you don't already.

So you can rest safe in the knowledge that Facebook will never see the hours you've spent looking at Hawaiian shirts for your dog.

More: **12 things you might want to delete from your Facebook page**

What did you think?

○ Vote

Google Internet Latest

Indigenous voice backers ‘ashamed’ as Australian voters back ‘no’ in referendum

Politics

Everybody Wanted To Date Her In The 80's & This Is Her Recently

One Daily | Sponsored

Introducing The Fully Electric Volvo EX90

FrequentSearches | Sponsored

She Was The Dream Girl In The 80s, This Is Her Now

Witty Reporter | Sponsored

She Was The Dream Girl Of The 90s, Now It's Hard To Look At Her

Tummy Tuck Hippo | Sponsored

KSI vs Tommy Fury: Tommy Fury defeats another YouTuber on judge's scorecards

Sport

Expert shares how to survive a zombie apocalypse

Viral

McDonald’s facing criticism for giving Israeli soldiers free meals

News

How OnlyFans model cheated death despite her breast implants exploding

Celebrities

KSI vs Tommy Fury: Ringwalk time revealed and how you can watch online

Sport

Jake Paul wants to ‘decapitate’ KSI after Sidemen star's defeat to Tommy Fury

Sport

Woman reveals the controversial question she asks on every first date

Tiktok

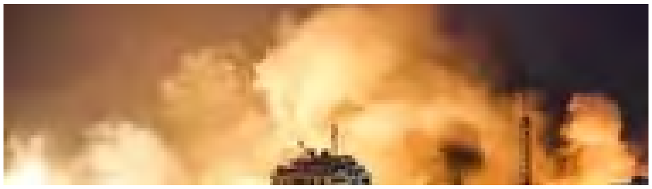
This Morning 'wants married couple' after Willoughby exit – Twitter has some ideas

Tv

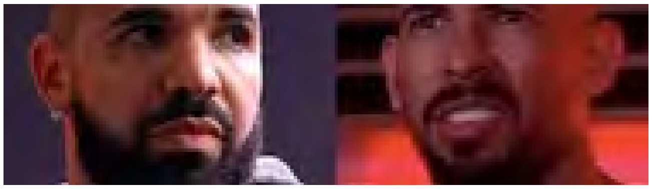
‘Amazing sight’ as pod of dolphins swim down Cork river at sunset

Pa Ready

Top 100



1



2

The Israel-Gaza Conflict Has Unleashed Social Media Misinformation

Israel

1 vote • 6 days ago

Drake Is Going In On Andrew Tate Over Comments About Canadian Men

Drake

• 6 days ago

3

Scientists Find 'Giant' Dinosaur Spider Fossil In Australia

Fossils

54 votes

4

Mother Of German Woman Paraded By Hamas Reveals How She Was Captured

Israel

2 votes

5

Intruder Storms Stage And Covers Labour Leader Keir Starmer In Glitter

Keir Starmer

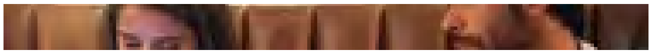
1 vote

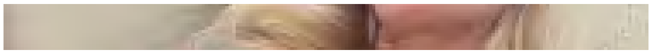
6

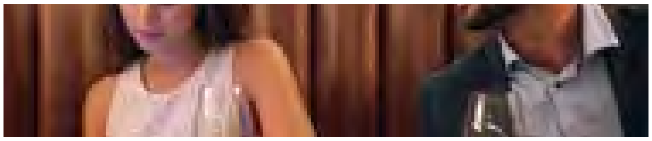
First Map Of Earth's Lost Continent Has Been Published

Zealandia

39 votes





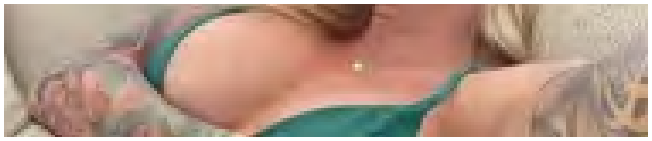


7

The Biggest Dating Phone Faux Pas According To Hinge

Relationships

20 votes



8

Woman With Two Vaginas Opens Up About What She Uses Each One For

Onlyfans

19 votes

9

Retiring Man Barely Gets A Farewell From Company – But There's A Happy Ending

Fundraiser

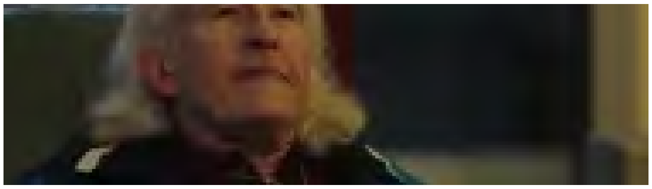
18 votes

10

Woman Loses Her Job After Xenophobic Train Rant Goes Viral

Xenophobia

16 votes

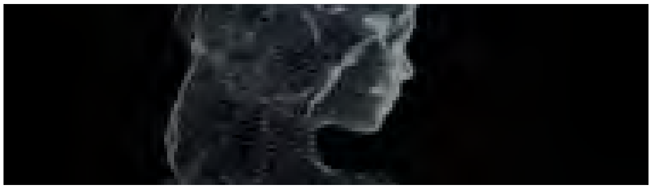


11

Steve Coogan Is Unrecognisable As Jimmy Savile In Gritty New BBC Drama

Jimmy Savile

15 votes

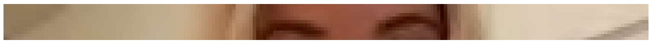


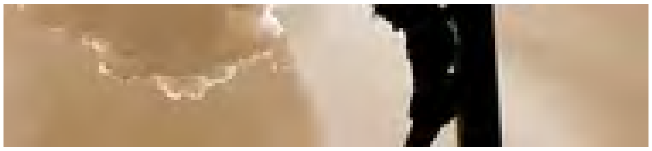
12

This Optical Illusion Is Seriously Confusing People

Optical Illusion

14 votes



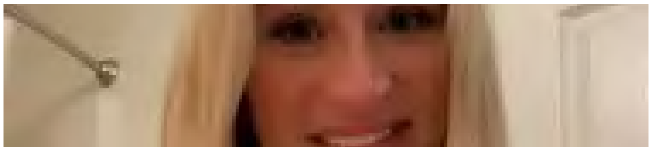


13

Scholar Argues That Jesus Was Actually A Hallucinogenic Mushroom

Jesus

13 votes

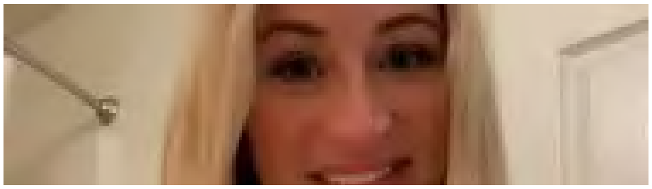


14

Teacher Who Had OnlyFans Side Hustle Placed On Leave By School

Onlyfans

13 votes

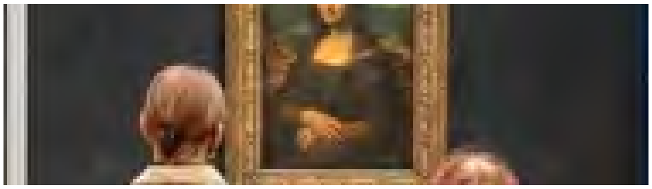


15

Teacher Who Had OnlyFans Side Hustle Placed On Leave By School

Onlyfans

13 votes

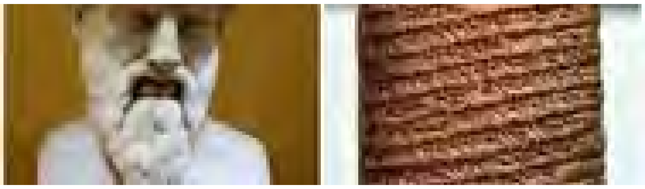


16

Scientists Unearth A Secret Hidden Within The Mona Lisa

Mona Lisa

12 votes



17

Pythagoras' Theorem Was Being Used 1,000 Years Before He Was Born

Pythagoras

18

A Hidden Underground Ocean Could Be Causing 'Slow-Motion' Earthquakes

Earthquake

12 votes

11 votes

19

12 Best Reactions To Steve Coogan's Ghoulish Jimmy Savile Portrayal

Steve Coogan

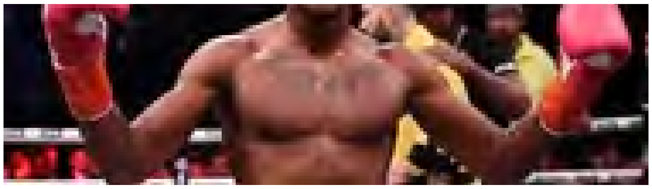
9 votes

20

Logan Paul Insists Danis Fight Still On After Violent Press Conference

Logan Paul

8 votes



21

Inspired By KSI? 5 Tips From An Expert On Getting Into Boxing

Boxing

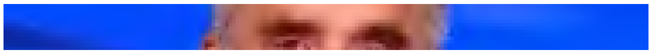
7 votes

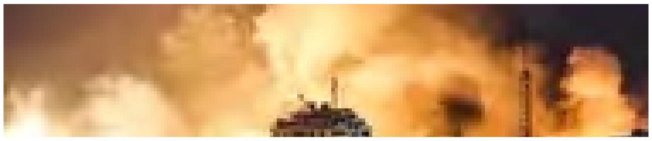
22

EuroMillions Winner Who Bought And Renovated Dream Estate 'Immensely Proud'

EuroMillions

7 votes



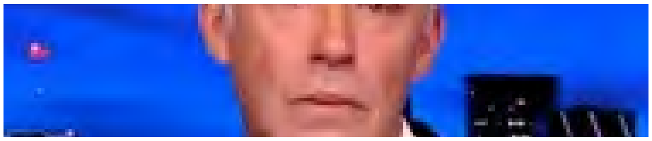


23

The Israel-Gaza Conflict Has Unleashed Social Media Misinformation

Israel

7 votes



24

Jordan Peterson In Tears Again During Piers Morgan Interview

Jordan Peterson

7 votes

25

Study Suggests Even Basic Worms Can Experience Human-Like Emotions

Animals

6 votes

26

Woman Catches Boyfriend 'Cheating' On Google Maps

Google Street View

6 votes

27

Norwich City's Nod To World Mental Health Day Is Heartbreaking

Mental Health

5 votes

28

Mum Shares Harrowing Warning After Daughter Killed By Birthday Balloon

Balloon

5 votes

Coin hoard belonging to Highland clan chief discovered

29

Mother Of German Woman Paraded By Hamas Reveals How She Was Captured

Israel

5 votes

30

Coin Hoard Belonging To Highland Clan Chief Discovered

Archaeology

5 votes

31

Beautician Mortified Over The Worst False Eyelashes She's Ever Seen

Eyelashes

5 votes

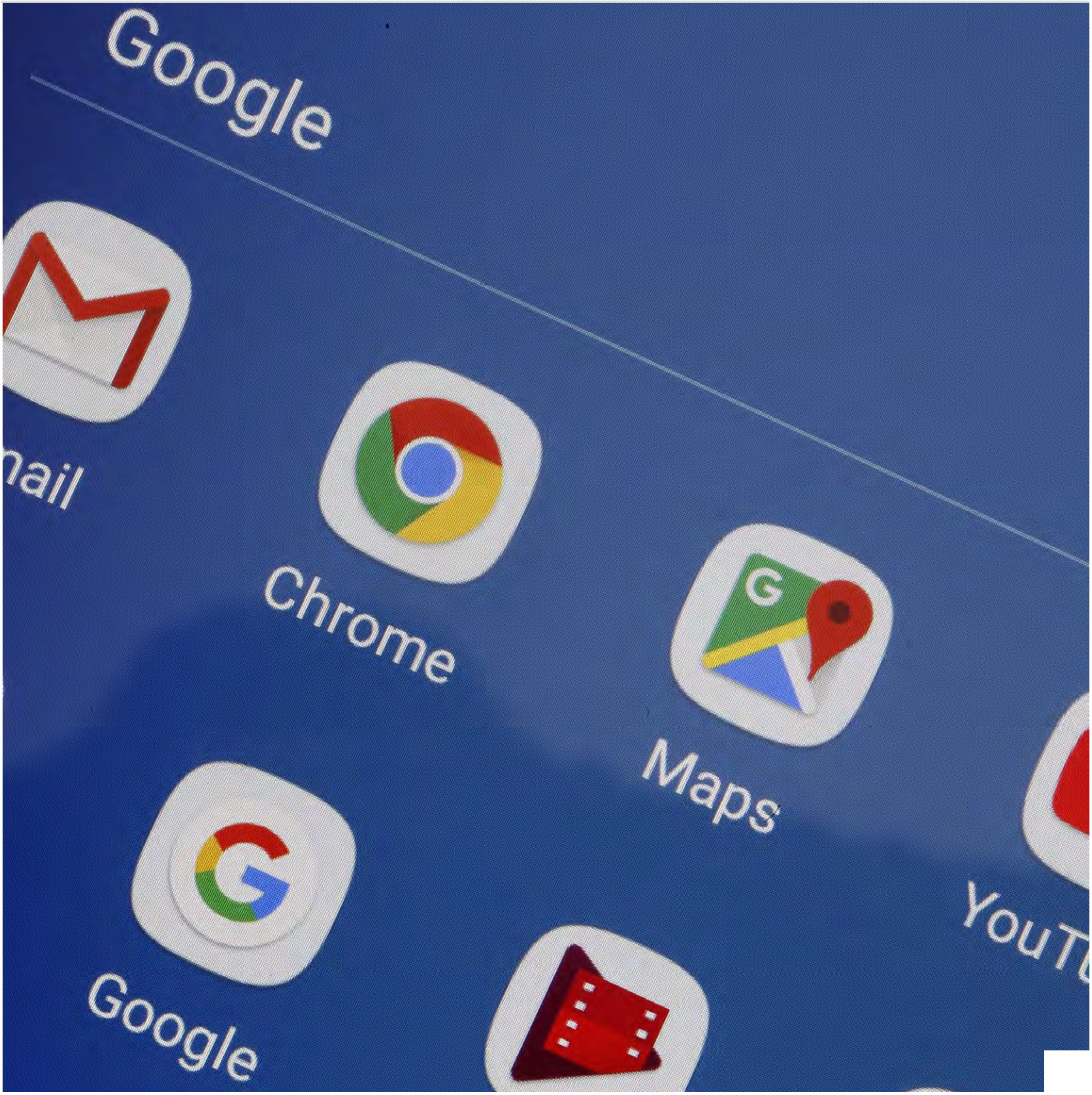
32

Airbnb Guest Squats At Home For 500 Days And Demands Money To Relocate

Airbnb

5 votes

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #713



Getty Images

Entertainment

Sorry, but Google Chrome Incognito isn't as private as you think

Did you know this?

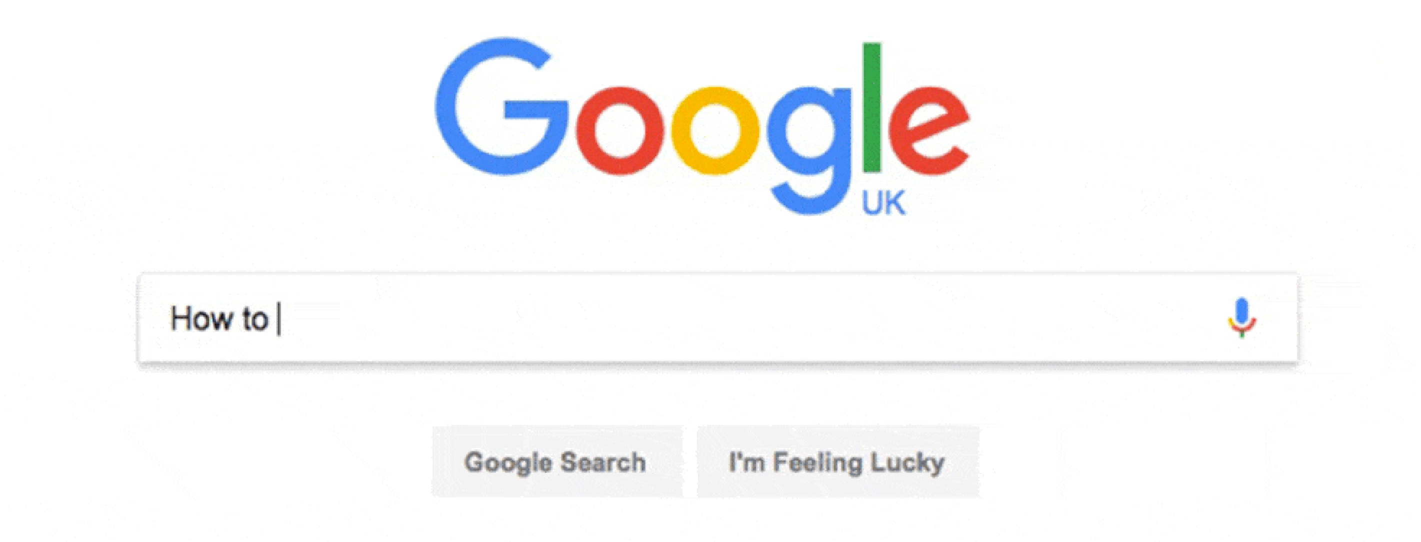
PUBLISHED: 16 APRIL 2019

Like everyone, we turn to the internet with our deepest, darkest questions. From 'is my vagina normal?' to 'Can you die from a hangover?', search engines are our best friends when it comes to getting the answers we need.

But if you've ever turned on 'Incognito Mode' in an attempt to hide your searches and hope it helps them stay off the internet, you're going to be in for a bit of a shock.

According to Indy100, 'Incognito Mode' actually only hides traces of your online activity from those using that specific computer, as opposed to the internet as a whole. So while it blocks third-party cookies - and stops your activity ingraining itself into your internet history - it has little effect on your ISP.

On top of this, 'Incognito Mode' doesn't stop websites being able to follow your activity, meaning that companies can still track wherever you visit on the internet and what you're searching, *even* if you're trying to keep it private.



How to |

Google

A study from Vanderbilt University also revealed that Google can still record the websites you browse while in Incognito Mode on the Chrome browser and link them to your identity, *if* you're logged into your Google account.

"While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user’s personal credentials stored in their Google Account," the study explained.

Getty Images

There goes any hope of 'privacy', then.

Related Story

You now have to be asked to be in Whatsapp groups

Related Story

Amazon admits staff listen to Alexa conversations

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #714

This article was published more than **4 years ago**

The Washington Post
Democracy Dies in Darkness

CONSUMER TECH

Help Desk: How to fight the spies in your Chrome browser

Our tech columnist answers your questions about how to protect your privacy while using Chrome, the most popular Web browser.

By Geoffrey A. Fowler

June 27, 2019 at 8:00 a.m. EDT

Is your Web browser spying on you? My recent column about the stark privacy differences between Google Chrome and Mozilla Firefox generated a lot of conversation — and questions from readers about what you can do to avoid surveillance while you surf.

The main lesson: If Google is a data vampire, Chrome is its fangs. For most people, not using a browser made by an advertising company is the simplest way to protect your data from thousands of tracking firms, including Google itself. I recommend switching to the nonprofit Firefox, which has privacy-focused default settings that automatically block tracking cookies from ad and data companies, including Google itself. Apple's Safari and Brave (which has an ad blocker built in) are also fine choices.

But I understand some people just can't quit Chrome. Barbara Karpel of Lauderhill, Fla., writes that her dental office uses software that asks for the Google browser. "When we submit a claim online, we are told that the insurance company's platform only accepts Chrome," she says.

Some people have invested in Chromebook laptops built around Google's browser — or just think Chrome is faster than the alternatives.

There *are* ways to defang Chrome, if you don't just use the default settings. Making Chrome better respect privacy requires messing around under the hood and installing privacy software, or extensions, into the browser.

Here's what I recommend to fight the advertising surveillance machine. Bonus: Some of these steps will also make websites load faster. Privacy for the win!

Don’t count on Incognito mode to protect your privacy. Or a VPN.

First, a warning: The “private” browsing mode in Chrome probably doesn’t do what you think it does. Incognito is the privacy equivalent of using an umbrella in a hurricane. It keeps information from being saved on your computer’s search and browsing history, which is only useful if you want to hide your activity from other people who share your browser. It does not stop websites, search engines and Internet service providers from tracking what you do.

“Does using a VPN solve the privacy issues you spoke about on Google Chrome?” asks reader Dan Harmon. Unfortunately, no. A VPN, or virtual private network, can obscure what you do online from your Internet service provider, including your work, school or someone spying locally on your network. But if you’re logged into Google or Facebook, a VPN won’t stop the tech giants and their partners from tracking your searches and other things you do in Chrome.

Tell Google to collect less personal information

A great place to start is by telling Google itself to stop some of the tracking of your online activity that it associates with your Google account. I suggest checking two spots:

Log in to Google’s advertising settings (adssettings.google.com), and make sure “ad personalization” is set to “off.” Doing this will make Google stop targeting ads to you on sites such as YouTube, though it alone won’t stop Google from collecting data about you.

Then head over to your Activity controls (myaccount.google.com/activitycontrols) and turn off — or set to “pause,” in Google’s strange lingo — your “Web & App Activity.” This tells Google not to record your searches, ads you click on, apps you use and other data about how you use its services. The downside, as Google will remind you, is that some of its services might not work as well. While you’re in this menu, go ahead and also pause “Location History” as well as “Voice and Audio Activity.”

Make sure you’re not using Chrome Sync

In your Chrome browser, tap the circular icon in the top right corner to make sure you’re not signed in with your Google account and using the Sync function. This would allow Chrome to pass your browsing history to Google. (The data would be private if you also set a passphrase in Chrome, but most people haven’t done that.)

While you're at it, tell Chrome not to automatically log in the browser to your Google account whenever you sign in to Gmail. To do that, tap the three dots in the upper right corner of Chrome to find your way to Settings. There, search "Gmail," and you'll find a setting for "Allow Chrome sign-in." Set that to "off."

There is one Chrome setting that privacy advocates disagree on: sending a "Do Not Track" request with your browsing traffic. Once upon a time, this was a good idea — but the industry hasn't taken action on it, and now some data companies actually use it as one more way to track people. The argument for turning it on: You're telling sites you specifically do not consent to them tracking you.

Add a privacy extension

You can download software to add to Chrome that works behind the scenes to automatically block tracking cookies and other snooping techniques used by an armada of ad and data companies.

These free programs work as extensions (also known as plug-ins) for the desktop version of Chrome. I have long used Privacy Badger, which works with minimal hassle and is backed by a nonprofit that is squarely on our side, the Electronic Frontier Foundation. Other good choices include DuckDuckGo and Disconnect, as well as Ghostery and uBlock, which block both trackers and ads.

Blocking trackers is more of an art than a science, so don't be afraid to try a few of them to see which work best on the sites you use most often.

In addition to protecting your privacy, the extensions could help sites load faster because they scrape tracking code out of pages.

Protect Chromebooks, too

"I downloaded Firefox," writes Eva Hashemi from Boca Raton, Fla. "Then my son reminded me that his new laptop is a Chromebook. Yikes! Any advice on this? It's too late to return it."

All hope is not lost. If your Chromebook isn't locked down (say, by school administrators) and you can still add extensions, you could install the privacy software I recommended above.

Or another idea: If the version of Chrome OS you're using supports the installation of Android apps, then you could also install the Android version of Firefox via the Google Play store.

Stop using Google for searches

Asks John Peterson from Atlanta: “If I use DuckDuckGo as my default, is my privacy maintained when using my Mac installed with Chrome?”

Using a privacy-first search engine such as DuckDuckGo won’t stop websites you visit from tracking you.

But changing your search engine to DuckDuckGo will definitely send less of your data to Google. Our searches are perhaps the most valuable personal information we share with Google — they convey not only what’s on our minds, but also what we’re looking to buy.

Chrome lets you switch your default search engine away from Google. Go to Settings, and then search for “search engine” and change the address bar setting.

DuckDuckGo is among the most well-known in the niche world of Google search alternatives. It promises not to track your searches or build a profile of you. It makes money through advertising around the context of what you search, rather than by tracking you.

Is it as good as Google? No. But it keeps getting better — and now claims over 41 million searches per day, up from 12 million in 2016. Clearly, interest in privacy is on the rise.

Read more tech advice and analysis from Geoffrey A. Fowler:

Don’t smile for surveillance: Why airport face scans are a privacy trap

Not all iPhones are the same. These cost less and are better for the Earth.

Rock this way: AirPods, Beats and Bose wireless ear buds take the headbang test

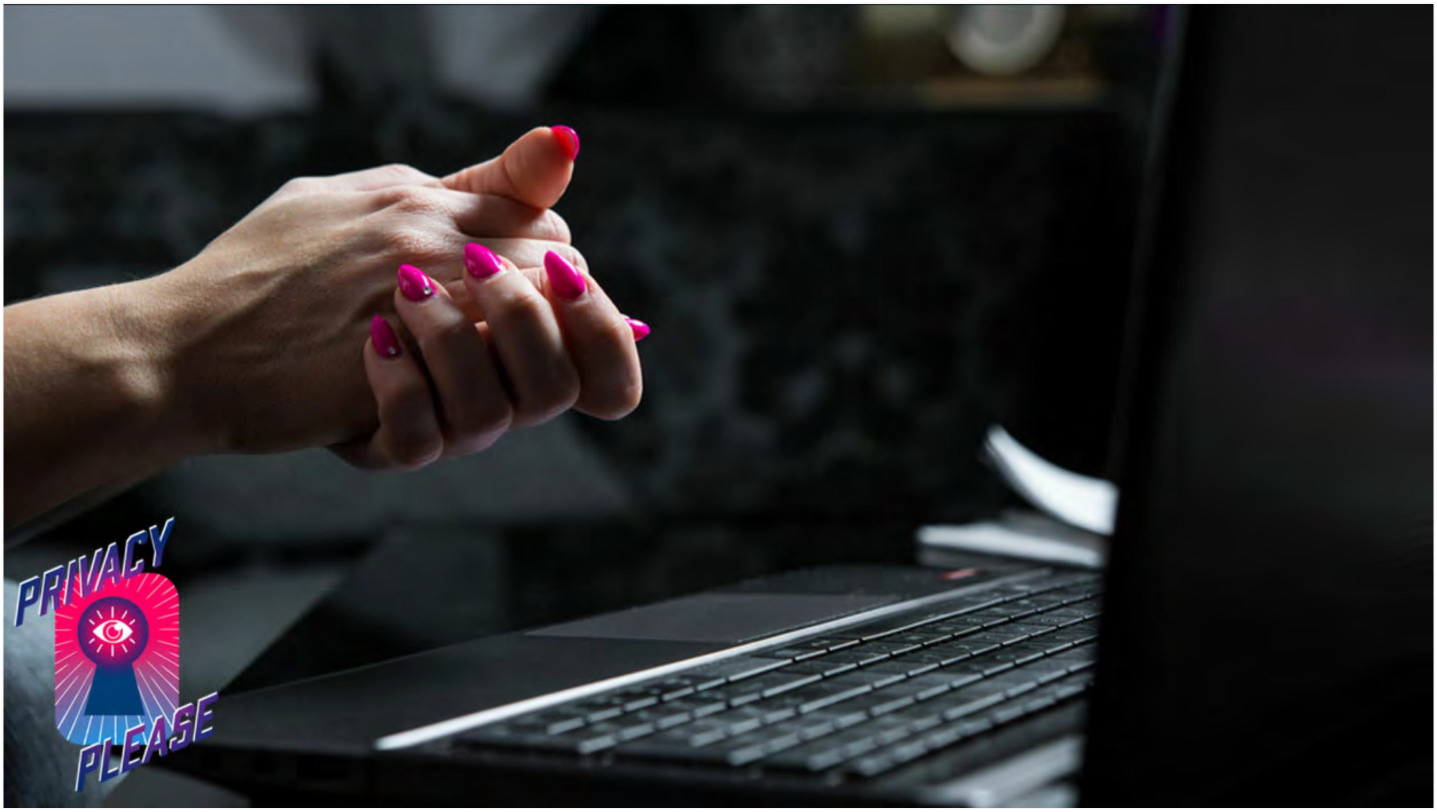
PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #715

Home > Tech

No, Incognito mode won't keep your porn habits private. This will.

A new study reveals that porn sites are leaking user data to third parties. Here's how to fight back.

By Jack Morse on July 18, 2019



Wipe it clean. Credit: SEBASTIAN GORCZOWSKI / GETTY

Privacy Please is an ongoing series exploring the ways privacy is violated in the modern world, and what can be done about it.

Your dumb privacy tricks aren't working. They still know what kind of porn you're watching.

So concludes a not-so-surprising study, which determined that online pornography sites are loaded with various trackers that leak private details about their users to third parties. And no, the study authors take pains to insist, Google's Incognito mode won't keep your secrets.

This latter point highlights broad confusion among the general public about what the Google Chrome feature actually does. Many people believe it renders their online browsing private, when in reality it just prevents Chrome from "[saving] your browsing history, cookies and site data, or information entered in forms."

Importantly, Google warns users, when using Incognito mode "[your] activity isn’t hidden from websites you visit, your employer or school, or your internet service provider."

Which brings us back to porn. The study, conducted by researchers hailing from Microsoft, Carnegie Mellon University, and the University of Pennsylvania, found a significant majority of pornography websites — 93 percent of the 22,484 analyzed — "leak user data to a third party."

And it gets worse. "Our content analysis of the sample’s domains indicated 44.97% of them expose or suggest a specific gender/sexual identity or interest likely to be linked to the user," continues the study.

In other words, your specific — and perhaps extremely private kinks — stand a pretty good chance of becoming not so private.

To illustrate this, the study authors lay out what for many is an all too familiar scenario.

"The websites [hypothetical porn consumer 'Jack'] visits, as well as any third-party trackers, may observe and record his online actions," explains the paper. "These third-parties may even infer Jack’s sexual interests from the URLs of the sites he accesses. They might also use what they have decided about these interests for marketing or building a consumer profile."

Once companies have said profile on this unsuspecting porn consumer, continues the study, they "may even sell the data."

This is problematic for all kinds of reasons, in addition to the skeevy factor alone. If your porn consumption reveals sexual preferences that are banned or outright illegal in repressive countries, this sort of tracking could literally threaten your physical safety.

Thankfully, there *is* a way to watch porn anonymously online. It's called Tor, and if it's not your best friend already, that should change today. Tor is an incredibly easy to use free service that keeps your identity private while browsing online.

There's even a Firefox-based Tor browser, which means the only real technical skills you need to browse privately are the ability to download (and update) a browser.

SEE ALSO: You should cover your phone's selfie camera, too →

Oh, but there is one *tiny* catch: you can't go full-screen any more. That's right, it's only the default window-size setting for your porn viewing from now on. This small tradeoff is made necessary because of a type of tracking, known as browser fingerprinting, that uses a computer's unique hardware and software settings to essentially fingerprint unique devi▷. Maximizing a browser window, which reveals some display features, helps in that process.

So there you have it: ditch the worthless Incognito mode, use Tor, and browse all that glorious internet porn to your heart's content. Hey, you can even use Tor for things *other* than viewing porn — after all, privacy is sexy.

Featured Video For You

Here's 5 tips for Spring cleaning your digital footprint

Topics Cybersecurity Porn Privacy

Jack Morse

Professionally paranoid. Covering privacy, security, and all things cryptocurrency and blockchain from San Francisco.

More from Privacy Please

Why you need a secret phone number (and how to get one)

07/14/2022 By Jack Morse

How to blur your house on Google Street View (and why you should)

05/27/2022 By Jack Morse

How to stop Spotify from sharing your data, and why you should

04/05/2022 By Jack Morse

How to make your Gmail account self destruct, and why you really should

01/02/2022 By Jack Morse

Your cute pet camera may hide a troubling secret

11/03/2021 By Jack Morse

Recommended For You

Get a $25 Amazon credit for buying paper towels and laundry detergent

3 hours ago By Tabitha Britt

Nation's first guaranteed income program for Indigenous parents launches in Washington

10/12/2023 By Chase DiBenedetto

Treat yourself to a Coleman tent and more Prime Day outdoor deals

10/11/2023 By Stacia Datskovska

Period care brands are reimbursing your tampon taxes. Here's how to cash in.

10/11/2023 By Chase DiBenedetto

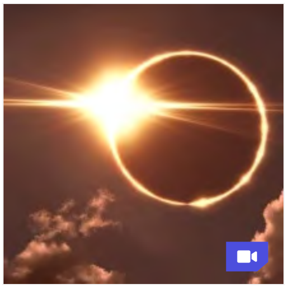
Treat yourself to all the best Prime Day beauty tech deals

10/11/2023 By Stacia Datskovska

Trending on Mashable

There's a solar eclipse Saturday — but don't take photos of it with your phone

10/13/2023 By Kimberly Gedeon



NYT Connections today: See hints and answers for October 16

17 hours ago *By Mashable Team*

Wordle today: Here's the answer and hints for October 16

9 hours ago *By Mashable Team*

Why are cafes, restaurants, and even towns banning influencers?

10/14/2023 *By Meera Navlakha*

Huberman husbands and the rise of self-optimization

10/13/2023 *By Christianna Silva*

The biggest stories of the day delivered to your inbox.

Email Address **Subscribe**

This newsletter may contain advertising, deals, or affiliate links. Subscribing to a newsletter indicates your consent to our Terms of Use and Privacy Policy. You may unsubscribe from the newsletters at any time.

TECH

SCIENCE

LIFE

SOCIAL GOOD

ENTERTAINMENT

BEST PRODUCTS

DEALS

About Mashable

Contact Us

We're Hiring

Newsletters

Sitemap

GROUPBLACK

Mashable supports **Group Black** and its mission to increase greater diversity in media voices and media ownership. Group Black's collective includes **Essence**, **TheShadeRoom** and **Afro-Punk**.

About Ziff Davis

Privacy Policy

Terms of Use

Advertise

Accessibility

Do Not Sell My Personal Information

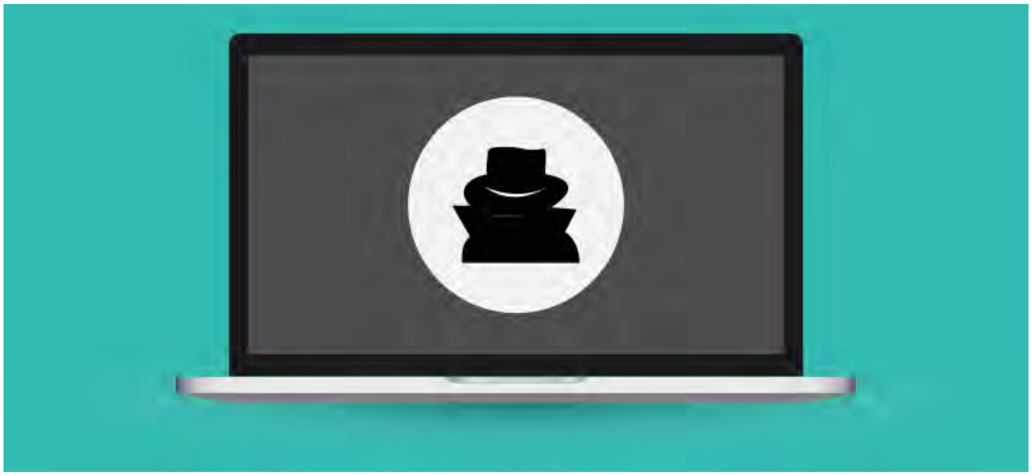
PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #716

United States {CYBERSECURITY} Magazine
A Multi-Platform Publishing Portal

Privacy

Incognito Mode: Are you Really Incognito?

Isabell Gaylord



Introduction

A lot of people have a wrong impression of Incognito Mode. Some users think this browsing mode covers your tracks completely from anyone, including both other computer users and the government. However, in reality, Incognito Mode is simply a way to keep your browsing history hidden. Additionally, Incognito Mode ensures that you log off of public computers without the computers storing your data.

Why Do People Use Incognito Mode?

People track out online information for multiple reasons. They track us for our safety and for other people's safety. Additionally, commercial entities track our activities in order to serve targeted ads. This is one of the reasons why every time you look up edubirdie on Google, you start receiving emails offering Boom Essays review article. However, the main reason is that our ISP just want to make sure we are not using their bandwidth to perform illegal activities.

Most regular internet users just want to spend a few hours on Facebook, or enjoy a Flat Earth YouTube video without being dragged into a Youtube hole of propaganda and Info Wars products. Yet, some use the internet as a gateway to criminal activities. In that respect, browsing history and cookie tracking is a reasonable endeavor. However, for this article we will focus on honest people interested in what Incognito Mode can do for them.

On the Subject of Cookies

In the online world, Cookies represent small pieces of textual information. These cookies hold various types of information regarding your browsing history. Cookies contain your login information, which is why most browsers keep your accounts active until you decide to logout. Cookies are also the reason why you don't have to fill out some forms such as country of origin or home address.

Incognito Mode clears all cookies that your browser gathers during a session. This keeps your web activities private from other users on the same computer. This way, nobody in your household would receive targeted ads based on your recent search or browsing history. More importantly, if you enter your login information on some website, Incognito Mode makes sure you won't stay logged in. Additionally, it will make sure your login information will not store on that computer. This is especially important when using a public computer, or someone else's with whom we don't want to share our private data.

Using Google Account During Incognito Mode

Google is the world's largest digital advertising entity, with billions of daily users via dozens of Google apps and services. As we already stated, Incognito Mode handles your privacy by dealing with the cookies and browsing history. However, is Google kind enough to do so as well?

When you use any Google service like Gmail, YouTube, or any other in the wide array of services this techno giant provides, you send all of your web-related data to Google. Therefore, it's important to know that hiding your internet activities from Google is only possible if you do not use and of your Google accounts.

Can Incognito Mode Hide Your Location?

This is a common misconception that results in a lot of people assuming that their online footprint is invisible. However, Incognito Mode is not a VPN tool, which means that any server you connect to will have information regarding your ISP, IP address, country of origin, etc. The only way one could hide such information is using a VPN software, or possibly using Tor browser or Opera. These programs allow you to hide your digital footprint and identity.

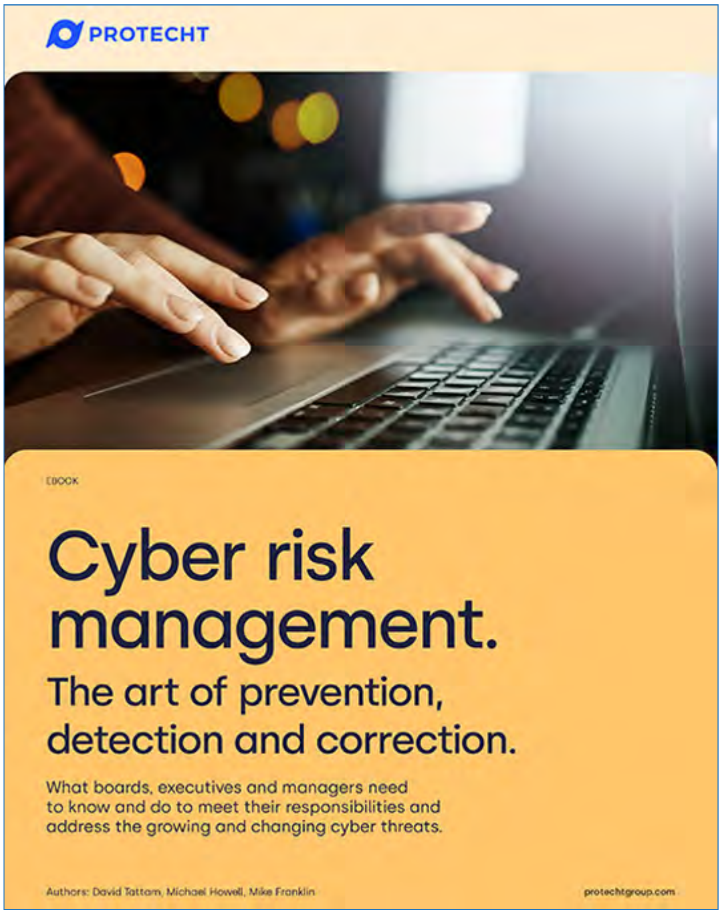
Conclusion

Incognito Mode is an excellent method of hiding your personal information from anyone else who is using the same computer as you do. Additionally, it is a smart way to avoid staying logged in while using public computers and networks. It's also a neat way to hide your browsing history from anyone who would frown upon some websites you are visiting.

However, it's important to remember that Incognito mode doesn't provide complete privacy. You can still leave a trace on your Google account if you log in during Incognito mode use. Furthermore, Incognito mode browsing is not the same as using a Virtual Private Network. Incognito mode can cover your tracks, but only from those in your immediate vicinity. Therefore, browse carefully.

Tags: Browsing, Google, Incognito Mode, Privacy, Social Media, Technology, VPN

CLAIM YOUR FREE EBOOK



Let Cyber Wise Guy bolster your cybersecurity and safeguard your business
Schedule a Free Consultation
CYBER WISE GUY

EVENTS CALENDAR

« OCTOBER 2023 »

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

BROWSE BY TOPIC

Engineering and Vulnerability Management

Training and Workforce Development

Industry & Business Best Practices

Data Storage and Access

Legal

RECENT POSTS

6 Signs You Need to Improve Your Enterprise Security

Left Shifting Mobile Security with DevSecOps

Safeguarding Personal Identity Information: Protecting Your Devices at Home and on Mobile Phones

AI and Privacy: Key Risks, Challenges, and How to Overcome Them

Are Viruses, Worms, and Malware The Same Thing?

Subscribe Log In Home Magazine Cybersecurity Channels Contact Us About Cyber Daily Calendar Resources Advertise With Us
Write for Us Privacy Policy

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #717

Private Browsing Won't Protect You From Everything

Private browsing gets rid of your browsing history, saved passwords, and field content. But if you think it keeps you safe from malware, ads, and ISP monitoring, think again.

By Ben Dickson

September 16, 2019

In the past several years, most internet browsers have added a private browsing mode aimed at protecting user privacy. Chrome calls it Incognito Mode; it's Private Browsing in Opera, Safari, and Firefox.

Characterized by dark-color themes and icons of masked figures, these modes can give a user the impression they're browsing anonymously. Researchers at the University of Chicago and Leibniz University of Hannover found that many users think private browsing will protect them against malware, advertising, tracking scripts, and monitoring by internet service providers (ISPs).

Nothing could be further from the truth. Here's what private browsing does and doesn't do.

What Does Private Browsing Hide?

Cookies, those bits of data stored in the browser that enable websites to keep track of user information, let you stay logged into your online accounts when you open your browser. For some websites, cookies also keep track of settings you configure, such as language, layout, and themes.

Private browsing is designed to avoid keeping traces of your browsing session on your computer. So when you open a private window, cookies from your main browsing window aren't carried over. And when you close the private browsing window, all cookies you generated during your session will be destroyed.

In theory, without cookies, websites can't identify you. So opening a new private browsing window should make you appear to the internet as a new user.

In practice, however, websites can still discover your identity by correlating other information, such as your IP address, device types, and browsing habits (time of day, pages visited, and so on). Private browsing hides *none* of that data. Big tech companies such as Facebook and Google have plenty of information about users, and by connecting the dots, they can identify you, even if you haven't logged into your account.

After you close a private browsing window, your browsing history, saved passwords, and the content you type in text fields (usernames, phone numbers, and so on) for that window is wiped. This means that the next person who sits behind your computer and fires up the browser will not be able to find out which websites you visited during your private browsing session.

But if you bookmark a page when you're in private browsing mode, it will be added to the bookmarks of your normal browsing page and will be visible to everyone. Also note that files you download to your computer while privately browsing will not be deleted when you close the window.

Can Your ISP See What You Search in Incognito?

This is one area in which private browsing won't protect you at all. Your ISP, corporate network administrator, and government agencies will be able to track your browsing habits regardless of the browsing mode you're using.

As your gateway to the internet, ISPs and network administrators control your traffic at the network level and can keep track of the websites you visit whether you're in normal or private browsing mode. Many ISPs share this kind of information with advertising agencies, which will, in turn, use the data to target you with relevant ads.

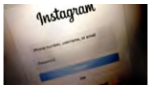
To hide your internet traffic from surveillance and monitoring, you can use a virtual private network (VPN). VPNs encrypt internet traffic and channel it through a third-party server, which then directs it to the destination. Your ISP will know you're using a VPN, but it won't be able to figure out which websites you're visiting.

Although VPNs protect you against ISP snooping, they sometimes collect and sell your information to other parties. So for absolute privacy, use the Tor browser. Tor encrypts your traffic and bounces it across several computers, called Tor nodes, before reaching its destination. None of the Tor nodes have full information about the source and destination of your internet traffic and can't spy on you. Tor is more private than VPNs, but it's also slower.

Private Browsing Does Not Stop Malware, Viruses

In the aforementioned study by the University of Chicago and Leibniz University, 25 percent of respondents said they believe private browsing protects them against malware and malicious websites.

RECOMMENDED BY OUR EDITORS



Facebook: We Stored Millions of Instagram Passwords in Plain Text

76 Percent of Parents Concerned For Children's Online Safety

But most malware will cause harm after it is installed on your computer, and malicious websites will harm you regardless of your browsing mode. For instance, when you open a phishing email and download a malware-infected attachment while browsing in private mode, you won't be protected (by your browsing mode). Also, private browsing won't protect you against malware already installed on your computer: a keylogger, for example, that silently monitors your keystrokes and sends them to a hacker's server.

To protect yourself against malware, you'll need an antivirus.

An exception to this is malicious extensions—the third-party features you add to your browser. Some hackers hide malware in browser extensions and do things such as steal your credentials or mine cryptocurrencies. Edge, Chrome, and Opera disable extensions by default, which will protect you against malicious browser extensions that might have found their way to your browser. Other browsers won't disable extensions in private browsing, but it takes only a few clicks to do it manually, and it's considered a good privacy practice.

Private browsing is a very useful and handy tool for a quick surfing session that will not leave traces on your computer. With a few caveats, it will protect your privacy against other people who use your computer and reduce some of the information you reveal about yourself when visiting websites.

But private browsing won't make you anonymous and won't protect you against surveillance and big tech snooping. For that, you'll need true privacy tools.

4 easy things you can do to be more secure online — Clarification Please

36 People Reacted

Was this article helpful?

👍 Yes **28**

👎 No **10**

Conversation **1 Comment**

Log in Sign up

What do you think?

Sort by **Best**

bobbie

3 May, 2023

Say goodbye to online surveillance and censorship with the Utopia P2P browser. This browser guarantees complete anonymity and encryption of all your online activities without ever compromising your data. If you're ever faced with a blocked site, the web proxy function will come in handy, giving you...

See more

Reply ▪ 👍 1 👎 ▪ Share

Powered by OpenWeb

Terms | Privacy | Feedback

Popular in the Community

Prime Big Deal Days

ALL PRIME BIG DEAL DAYS COVERAGE

Latest Deals

- Walmart's 40+ Best Prime Day Deals: Sale Ends Today
- Last Chance: The Best Prime Day Deals You Can Still Get on Amazon Right Now
- Anti-Amazon Prime Day? Check Out These 33+ Best Buy Pre-Black Friday Deals
- Our Favorite Prime Day Video Doorbell Deals: Arlo, Blink, Ring, and More
- Best Amazon Prime Day Printer Deals: Save Now on Brother, Epson, More
- Serious Amazon Prime Big Deal Days Savings on Apple Gear
- Sweet Prime Day Deals on Robot Vacuums From iRobot, Shark, Eufy, and More
- 60 Last-Minute Fall Prime Day Deals You Can't Miss
- The Best Prime Day Laptop Deals: Save Big on Apple, Lenovo, Razer, and More
- The Best October Prime Day Deals Under $50 You Can Still Grab
- The Best Tablets of Prime Big Deal Days: Save on iPads, Galaxy Tabs, and More
- The Best Prime Day 2023 Gaming Deals: PS5, Xbox, and Switch Gear on Sale
- The 10 Most Popular Prime Day Deals You Can Still Get
- Get the Lowest Prices of the Year on Echo, Fire TV, Ring, and More
- The Best Prime Day Desktop PC Deals on Acer, Dell, HP, and More

Our Favorite Deals

About Prime Big Deal Days

Other Sales

FURTHER READING

Mozilla Is Adding a Fake Review Checker to Firefox

BY MATTHEW HUMPHRIES

Too Many Chrome Tabs? Google Preps Feature to Automatically Organize Them

BY MICHAEL KAN

Apple's Latest iPhon Pro Headache: Repo of Screen Burn-In

BY KEGAN MOONEY

TRENDING

T-Mobile May Move You Off Your Current Plan: Here's How to Stop It

BY ROB PEGORARO

Ring Mailbox Sensor Review

●●●◐○ 3.5

MIT Hypes Lunchbo Sized Robot Produci Oxygen on Mars

BY NATHANIEL MOTT

About Ben Dickson

Ben Dickson is a software engineer and tech blogger. He writes about disruptive tech trends including artificial intelligence, virtual and augmented reality, blockchain, Internet of Things, and cybersecurity. Ben also runs the blog TechTalks. Follow him on Twitter and Facebook.

Read Ben's full bio

Read the latest from Ben Dickson

- What Is Deep Learning?
- What Is Artificial Intelligence (AI)?
- What Is Spatial Computing? A Basic Explainer
- What Is ChatGPT? A Basic Explainer
- This Technology Could Transform Humanity, If Silicon Valley Doesn't Ruin It
- More from Ben Dickson

PCMag Newsletters

Our Best Stories in Your Inbox →

Follow PCMag

HONEST, OBJECTIVE, LAB-TESTED REVIEWS

PCMag.com is a leading authority on technology, delivering lab-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

How We Test Editorial Principles

Reviews Best Products

Categories Brands

Events Series

Encyclopedia Sitemap

About PCMag Careers

Contact Us Press Center

askmen

EXTREMETECH

IGN

lifehacker

Mashable

Offers.com

RetailMeNot

SPEEDTEST

GROUPBLACK

PCMag supports Group Black and its mission to increase greater diversity in media voices and media ownerships.

About Ziff Davis

Privacy Policy

Terms of Use

Advertise

Accessibility

Do Not Sell My Personal Information

AdChoices

PLAINTIFF'S MOTION *IN LIMINE* 2; Google Exhibit #718

Google Chrome privacy: Can you trust the Incognito window?

By **Ben Dickson** - November 21, 2019

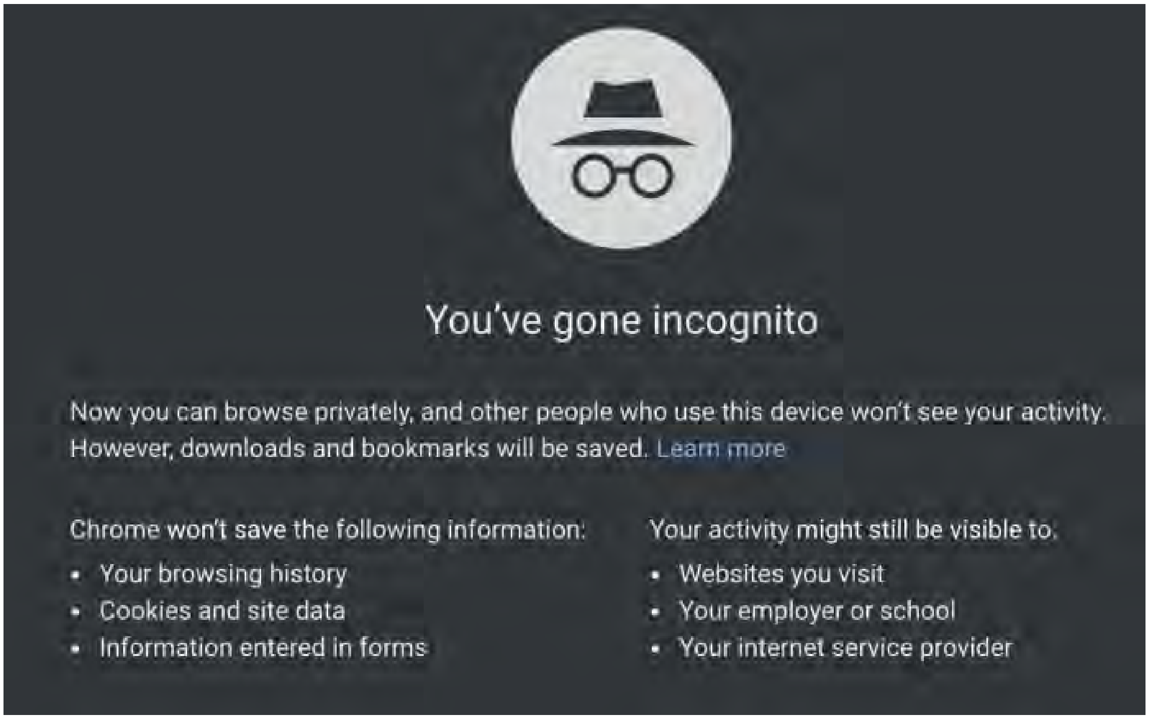
Image credit: Depositphotos

Privacy is fast becoming a hard-to-earn luxury. As you browse through websites, it's hard to shake off the creepy feeling that wherever you go, unseen eyes are watching you: Google, Facebook, your internet service provider, the government, the person sitting next to you, etc.

Among the many privacy-enhancing tools, one of the best known is the Chrome Incognito window, Google's version of private browsing. Incognito window provides a measure of privacy if you're browsing on a shared computer. But it's far from being a perfect solution.

Unfortunately, many people don't understand the privacy implications of Google's Incognito window and end up sity of Chicago and Leibniz r private browsing windows will protect them against malware, advertising, tracking codes and the monitoring by connection gateways.

Here's what you need to know about the privacy features and the limits of Chrome's Incognito window.



You’ve gone incognito

Now you can browse privately, and other people who use this device won’t see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won’t save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Google Chrome’s Incognito window will protect your activity against other people using your device

Interestingly, Google clearly spells out everything you can expect from Incognito mode when you open a new private window. According to Google, “Now you can browse privately, and other people won’t see your activity.”

What does activity mean?

Browsing history: Google Chrome keeps track of the webpages you visit to make it easier for you to return to those pages in the future. Pressing CTRL+H on Windows (⌘+Y on macOS) shows all the webpages you’ve visited before.

Moreover, if you’ve synced your Chrome browser with your Google account, every page you visit will be registered in your online browsing history. This means that if you go to another computer and sync your Google account on a new Chrome browser, your browsing history will be transferred over.

webpages you visit after you
nputer won’t be able to look at
your browsing history.

Cookies and site data: Cookies are bits of data attached to websites that are exchanged between the browser and the web server. Cookies keep track of user sessions, site preferences, local settings and other vital functions of web applications.

Cookies are what enable websites to show different content to each user. When you log in to an online account, say Gmail or Facebook, the web server produces a cookie and sends it to your browser. The browser stores the cookie and resends it to the server on every new request (every time you click on a new button or link). The server uses the cookie to associate your application session with your user ID and serve content that corresponds to your user account.

Cookies also enable web service providers to track you across websites. When you browse to a website that has the Facebook Like and Share button or the invisible Facebook Pixel, Facebook uses your session cookie to trace you and later use the information to target you with advertising.

When you fire up a new Incognito window, none of your cookies are carried over. You can verify this by browsing to Facebook or Gmail. Even if you had logged in to your accounts before opening the Incognito window, you will still be redirected to the login page. Without the cookie, the website will treat you as a new user.

The privacy benefit of Incognito window is that you will be able to browse to different pages without traceable cookies (there's a caveat to this that I will mention later). Also, if you log in to any online account, closing the Incognito window will destroy the cookie associated with that session. Therefore, the next person who sits behind the computer won't be able to access the accounts you were using when in Incognito mode, even if you had forgotten to log out before closing the window.

Information entered into forms: Forms are text areas you see in pages that require you to fill in information, such as your name, username, email address, phone number, etc. When you enter information in a form. It then makes it available in other pages to make it easier for you to enter data in forms.

This feature can turn into a privacy issue, however, if you're using a public computer. Other people using the same Chrome browser will see your personal data when going to pages that have data forms.

The Incognito window deletes all information you entered in forms when you close it, which gives you better privacy on shared computers.

The privacy conditions of Google Chrome's Incognito window

Google also makes it clear that there are several areas where Chrome's Incognito window won't provide privacy.

Websites you visit: The easiest way for web applications to track users is to use cookies. But it is not the only way they can track you. Other bits of information can point to your device. For instance, I've seen some users use the

ide their identity. The premise is,

sociate their activity to their

account.

But Twitter also keeps track of IP address, device type, device ID and browser type and version. Technically, it will be able to use all those factors to link your activity to your account. Facebook goes further and even tracks your activity across other websites when you're not logged in to your account.

Your employer or school: If you're using a corporate or school network, all your traffic will be channeled through a gateway such as a router or server. The person who manages the gateway will have full visibility into your traffic, whether you're browsing with Incognito mode or not. They can filter the network's internet traffic based on IP addresses and keep track of your browsing habits.

Your internet service provider: The ISP is the company that gives you access to the internet. Think of it as the corporate network manager, but at a much larger scale. ISPs are also gateways, which means they will be able to trace all your browsing habits, regardless of whether you use private browsing or not.

Bookmarks and downloads: If you download anything while using the Incognito window, it will stay in your downloads folder after you close the window. Also, if you happen to bookmark anything while browsing in Incognito, the bookmark will be saved to your main browser. Keep that in mind.

Final words on privacy with Google Chrome’s Incognito mode

If you want to enhance your privacy when browsing with the Incognito window, consider using a virtual private network (VPN). VPN applications encrypt your internet traffic and channel it through a VPN server. This will hide your browsing activities from your local gateway or ISP. They won’t know which websites you browse to, but they will be able to detect that you’re using a VPN.

Overall, be careful: Chrome’s Incognito window is a good privacy tool when you have concerns about other users who have access your computer and browser. But that’s about as far as you can trust it.

Ben Dickson

Ben is a software engineer and the founder of TechTalks. He writes about technology, business and politics.

PLAINTIFF'S MOTION *IN LIMINE* 2;
Google Exhibit #719

Inc.

NEWSLETTERS SUBSCRIBE

TECHNOLOGY

Google Calls It Private Browsing. Oh, No It Isn't

It's such a tempting term, but please beware. There's very little that's private about it.

BY CHRIS MATYSZCZYK, OWNER, HOWARD RAUCOUS LLC @CHRISMATYSZCZYK

Not so private? Getty Images

Absurdly Driven looks at the world of business with a skeptical eye and a firmly rooted tongue in cheek.

Humans are dreamers. That's why we get into so much trouble.

Article continues after video.

We dream of a perfect life and even when we get it, we realize it's not so perfect at all. Oddly, two Ferraris don't make us happier than one.

For many people these days, however, one significant dream revolves around privacy. We want to believe we're not being spied upon with every breath we take and every move we make. We want to believe we're clever enough to achieve that.

A temptation to that end is to open our laptops, launch a browser and go, as Google terms it, *Incognito*. With that name, Google encourages us to believe that we can potter about the web and no one will know:

> *Now you can browse privately, and other people who use this device won't see your activity.*

How uplifting. You can do so many things without your beloved knowing. Like shopping for their gifts. Or, well, other things. Even Orwell would be impressed, right?

Well, except that if you read the smaller print fully -- and who does these days? -- Google is very clear just how private this form of browsing is:

First of all:

> *Downloads and bookmarks will be saved.*

Then there's this:

> *Your activity might still be visible to: Websites you visit, your employer or school, your internet service provider.*

Your employer? Your school? That really doesn't sound so good, does it? The truth is that private browsing is as private as our playing a video with the sound on at the airport.

It's always worth being careful in interpreting product names. The name *Incognito* implies that you can hide from prying eyes. The truth, though, is a little different. Or, indeed, entirely different.

It's not as if Google is alone in offering this kind of troubling misnomer. Firefox, for example, has so-called Private Windows. However, the non-profit explains:

> *Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.*

Easier. Relatively easy.

But in no way actually private.

DEC 8, 2019

The opinions expressed here by Inc.com columnists are their own, not those of Inc.com.

GLOBAL
RESEARCH
UNLOCKED™

PLAINTIFF’S MOTION *IN LIMINE* 2; Google Exhibit #720

DAVID NIELD SECURITY AUG 2, 2020 7:00 AM

Incognito Mode May Not Work the Way You Think It Does

Every browser has a private mode—but the privacy it offers has a limit.

ILLUSTRATION: ELENA LACEY

SAVE

NO MATTER WHICH browser you prefer—Chrome, Firefox, Edge, Safari, Opera, or any of the others—it will almost certainly offer an incognito or private mode, one which ostensibly keeps your web browsing secret. (Google Chrome still shows a hat-and-glasses icon when you go incognito, as if you're now in disguise.)

Incognito or private mode does indeed keep certain aspects of your browsing private, but it's important to be aware of what it hides and erases from your computer or phone and what it doesn't. Once you understand exactly what these modes do in your browser, you'll know when they can be most useful.

What Incognito Mode Does

Perhaps the easiest way to think about incognito mode is that as soon as you close the incognito window, your web browser forgets the session ever happened: Nothing is kept in your browsing history, and any cookies that have been created (those little bits of data that log some of your actions online) are promptly wiped.

Cookies are what keep items in your Amazon shopping cart even if you forget about them for days, for example, and they also help sites to remember if you've visited them before—which is why you normally only get pestered to sign up for a site's newsletter the first time you arrive. You might notice if you visit all your favorite sites in incognito mode, you won't get recognized, and are then asked to sign up for a whole load of newsletters and special offers all over again.

Chrome attempts to explain how incognito mode works when you open up a private session. SCREENSHOT: DAVID NIELD VIA GOOGLE

This sort of anonymity is what incognito mode is good at—it's like starting again with a blank slate, for better or for worse. Try loading up Twitter or Gmail, and these sites won't automatically log you in as they normally do. For the same reason, incognito mode can sometimes be a handy way of accessing more free articles from a paywalled site (the site won't instantly identify you as someone who's been before, although many paywalled sites use other methods to figure that out).

Your browser won't remember where you've been, what you've searched for, or the information you've filled into web forms while you've been in incognito mode—it's as if Chrome, Firefox, or whatever browser you're using has its back turned until you close down the incognito mode again.

With browsers now so personalized, you're probably familiar with your frequently visited websites appearing as you type into the address bar or search box. Anything you've visited or searched for while in incognito mode shouldn't appear in these suggestions (with a few caveats, as we'll mention below). You'll notice in some browsers that you can't pull the normal trick of reopening a tab you've just closed while in incognito mode—your browser has already forgotten that you ever opened it in the first place.

All modern browsers come with a private or incognito mode of some description. SCREENSHOT: DAVID NIELD VIA FIREFOX

Incognito mode certainly has its uses: You can sign into multiple accounts at the same time, for instance, rather than signing in and out. It's also helpful when you need to run a few quick searches on sensitive topics—like health issues—that you don't want to show up in your browsing or search history in the future.

While all traces of your incognito activities will be gone as soon as you close these windows, this is true only as far as your browser and the device you're currently using are concerned. These days, tracking and data mining extends way beyond a single browser and a single device.

What Incognito Mode Doesn't Do

As soon as you log into any of your favorite sites in incognito mode—Facebook, Amazon, Gmail—your actions are no longer anonymous or temporary, at least as far as those services are concerned. Although cookies and tracking data are deleted when your private session finishes, they can still be used while the session is active, linking your activities between various accounts and profiles.

That means if you're signed into Facebook, for example, Facebook might well be able to see what you're up to on other sites and adjust its advertising accordingly, even in incognito mode. Blocking third-party cookies in your browser can stop this to some extent (Chrome even offers you the option when you open incognito mode), but such is the reach of ad networks and tracking technologies that it's difficult to stop it entirely.

Sign into any of your accounts and you can easily be tracked, even in private mode. SCREENSHOT: DAVID NIELD VIA APPLE

Google has already been in trouble for this practice, though it's not alone. If you sign in to Google while using incognito mode, then your searches are once again being logged and associated with your account, assuming that's how your Google account preferences are set up—and Google is potentially also using its ad network and tracking technologies on other sites to keep tabs on you there too.

Even if you don't sign in anywhere, the websites that you visit can use various clues—your IP address, your device type, your browser—to figure out who you might be, and to tie this to other information that might already be associated with you. Certain browsers are fighting back against this type of tracking, called "fingerprinting," but it still goes on.

Any files you've downloaded in incognito mode remain on your system. SCREENSHOT: DAVID NIELD VIA GOOGLE

Incognito mode doesn't hide your browsing from your internet service provider or your employer, and it doesn't wipe out files you've downloaded. In other words, you need to think of it as a way of hiding your online activities from the particular browser on the particular device you're using, and from the other people using that device. When it comes to everything else, there are no guarantees.

The limits of incognito mode highlight just how hard it is to stay invisible on the web. To keep any tracking down to an absolute minimum, you need to pick a browser focused on privacy, use services like the DuckDuckGo search engine that don't mine your data, and deploy a reliable VPN program whenever you connect to the web. We've written more about the extra steps you can take here.

More Great WIRED Stories

- There's no such thing as family secrets in the age of 23andMe
- Inside Citizen, the app that asks you to report on the crime next door
- Mad scientists revive 100-million-year-old microbes
- How two-factor authentication keeps your accounts safe
- This algorithm doesn't replace doctors—it makes them better
- 👁 Prepare for AI to produce less wizardry. Plus: Get the latest AI news
- 🎙️ Listen to Get WIRED, our new podcast about how the future is realized. Catch the latest episodes and subscribe to the 📩 newsletter to keep up with all our shows
- 🏃‍♀️ Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers, running gear (including shoes and socks), and best headphones

David Nield is a tech journalist from Manchester in the UK, who has been writing about apps and gadgets for more than two decades. You can follow him on Twitter.

CONTRIBUTOR 𝕏

TOPICS PRIVACY BROWSERS CHROME FIREFOX

MORE FROM WIRED

How to Remove Your Personal Info From Google by Using Its ‘Results About You’ Tool

You can now set up alerts for whenever your home address, phone number, and email address appears in Search.

REECE ROGERS

Are You Being Tracked by an AirTag? Here’s How to Check

If you’re worried that one of Apple’s trackers is following you without consent, try these tips.

REECE ROGERS

A New Attack Impacts Major AI Chatbots—and No One Knows How to Stop It

Researchers found a simple way to make ChatGPT, Bard, and other chatbots misbehave, proving that AI is hard to tame.

WILL KNIGHT

China-Linked Hackers Breached a Power Grid—Again

Signs suggest the culprits worked within a notorious Chinese hacker group that may have also hacked Indian electric utilities years earlier.

ANDY GREENBERG

The Twisted Eye in the Sky Over Buenos Aires

A scandal unfolding in Argentina shows the dangers of implementing facial recognition—even with laws and limits in place.

KAREN NAUNDORF

Deepfake Porn Is Out of Control

New research shows the number of deepfake videos is skyrocketing—and the world's biggest search engines are funneling clicks to dozens of sites dedicated to the nonconsensual fakes.

MATT BURGESS

Rumors of a ‘Global Day of Jihad’ Have Unleashed a Dangerous Wave of Disinformation

The rapid spread of violent videos and photos, combined with a toxic stew of mis- and disinformation, now threatens to spill over into real-world violence.

DAVID GILBERT

The Israel-Hamas War Is Drowning X in Disinformation

People who have turned to X for breaking news about the Israel-Hamas conflict are being hit with old videos, fake photos, and video game footage at a level researchers have never seen.

DAVID GILBERT